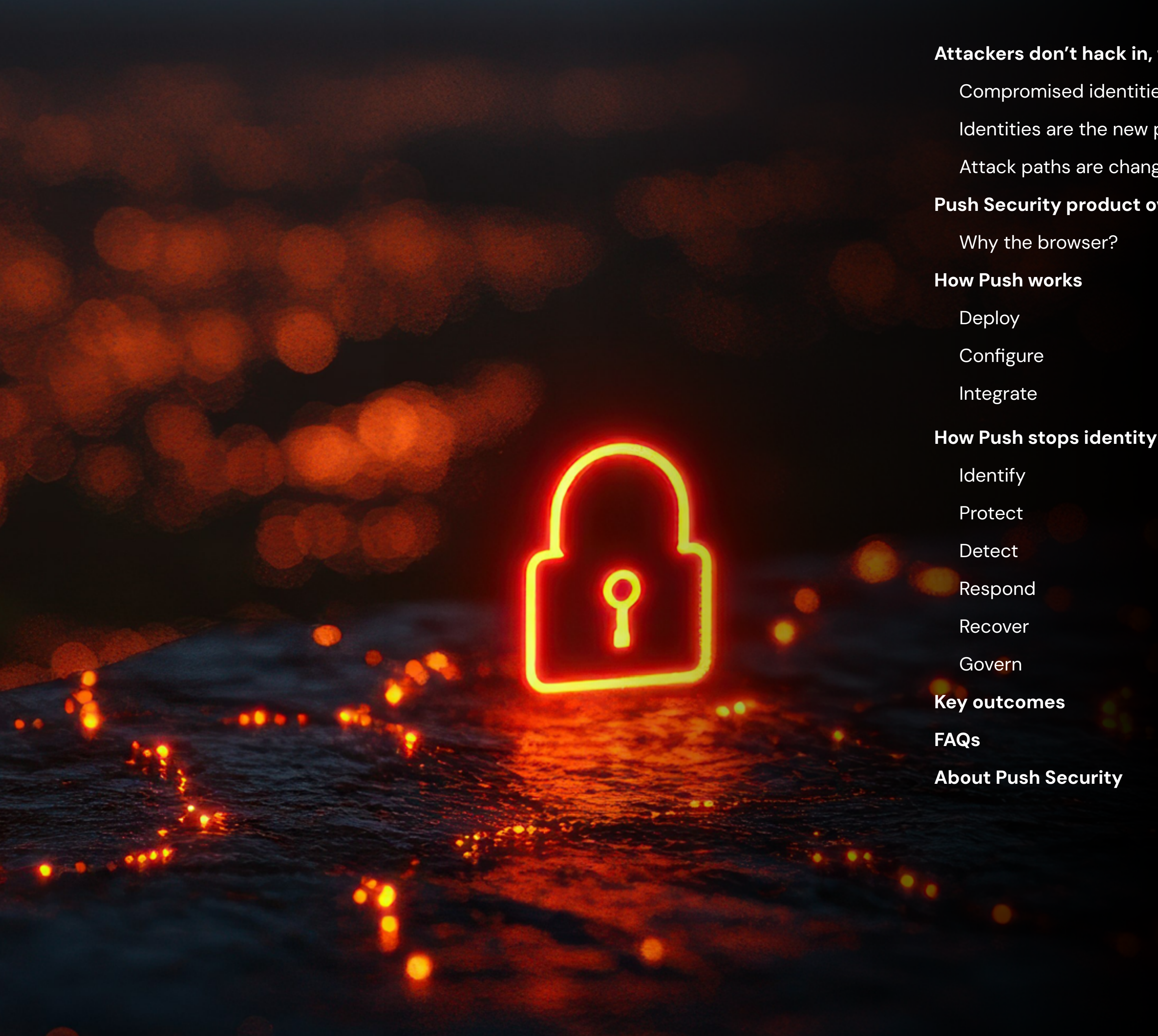
Push Security

Stop identity attacks & secure the new perimeter

Push Security product overview



Push Security

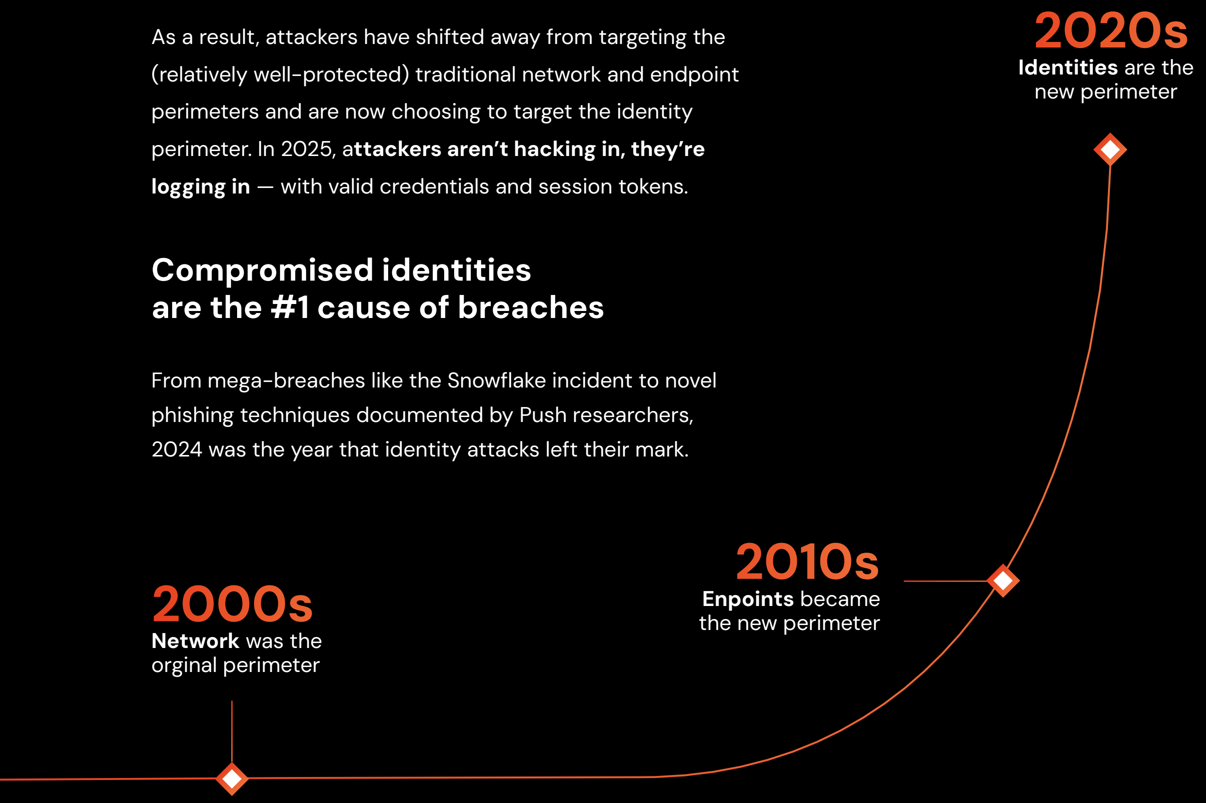
Attackers don’t hack in, they log in

Modern working practices using cloud services have left the typical organization with thousands of unmanaged workforce identities sprawled across the internet. These identities present attackers with a huge, largely unmonitored attack surface rich in vulnerabilities that can be exploited to compromise sensitive data and systems.

As a result, attackers have shifted away from targeting the (relatively well-protected) traditional network and endpoint perimeters and are now choosing to target the identity perimeter. In 2025, a**ttackers aren’t hacking in, they’re logging in** — with valid credentials and session tokens.

Compromised identities are the #1 cause of breaches

From mega-breaches like the Snowflake incident to novel phishing techniques documented by Push researchers, 2024 was the year that identity attacks left their mark.



2000s
Network was the orginal perimeter

2010s
Enpoints became the new perimeter

2020s
Identities are the new perimeter

75%
Of reported breaches use credentials and phishing
Verizon 2024 Data Breach Investigations Report

90%
Of businesses experienced an identity-related incident in 2024
IDSA 2024 Trends in Identity Security

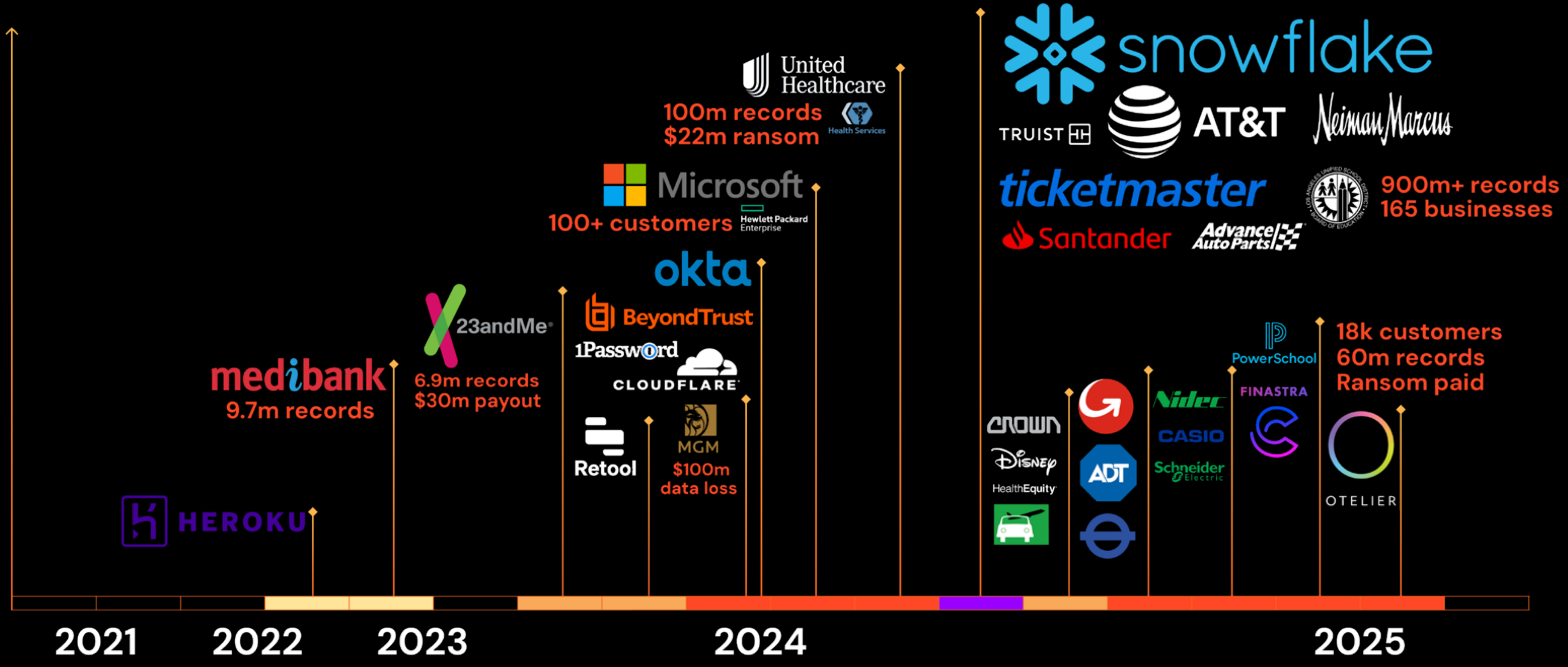
600 million
Identity attacks observed per day
Microsoft Digtital Defense Report 2024

146%
Increase in AiTM kits observed in ‘23/4
Microsoft Digtital Defense Report 2024

266%
Increase in infostealer activity in ‘23/24
IBM Threat Report 2024

39,000
Session token attacks detected per day
Microsoft Digtital Defense Report 2024

3 in 4 (73%) of public identity breaches in 2024 involved stolen credentials.



Identities are the new path of least resistance

Organizations now have thousands of workforce identities on hundreds of third-party applications. These form a vast, vulnerable and largely unmonitored attack surface for attackers to target.

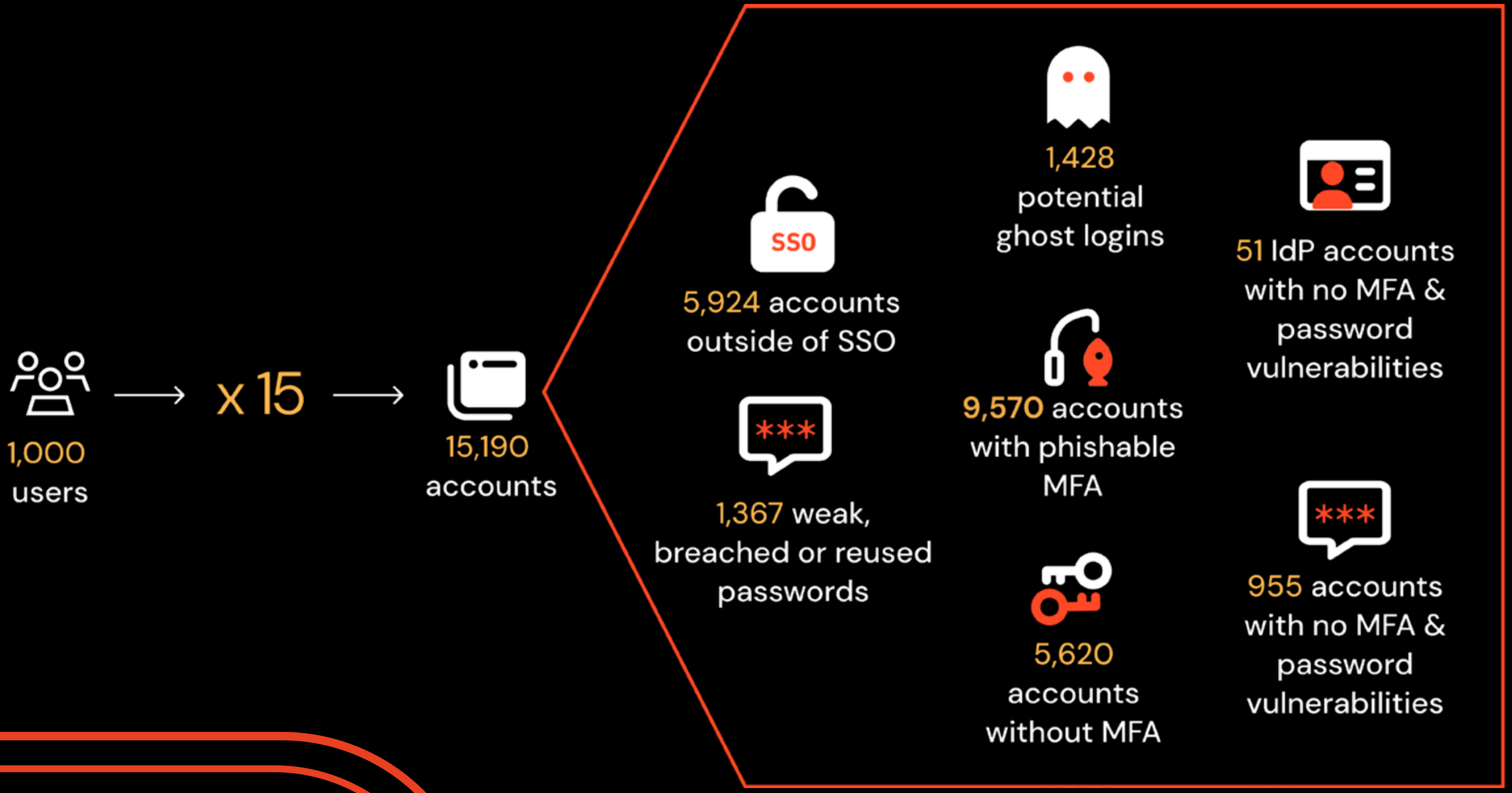
A Push review of 300,000 accounts among our customer base found that employees have on average 15 accounts each, and the vast majority are vulnerable to identity attack techniques.

To take advantage, attackers have developed TTPs to bypass traditional controls, evade detection and execute attacks faster than defenders can respond.

A few key trends:

- **Because attacks are taking place entirely over the internet, established network and endpoint controls like EDR, IDS, NAC, etc., are unable to intercept them.**
- **Established identity controls like SSO, MFA and password managers are failing to prevent identity breaches and continue to leave coverage gaps.**
- **Legacy IAM tools focused on a single identity store are failing to keep up with the sprawl of decentralized web identities.**
- **Email-based anti-phishing controls are being routinely defeated by modern phishing kits designed to evade them, and attacks have expanded far beyond the inbox, taking place over IM platforms, social media, and just about everywhere on the internet.**
- **This leaves you mainly reliant on application logs from the SaaS services themselves — but these are often not provided at all, have key gaps (e.g. authentication) or cannot be programmatically ingested for detection and response due to the format/mechanism.**

How many vulnerable identities are there in a 1,000 seat organization?



1,000 users → x 15 → 15,190 accounts

5,924 accounts outside of SSO

1,367 weak, breached or reused passwords

1,428 potential ghost logins

9,570 accounts with phishable MFA

5,620 accounts without MFA

51 IdP accounts with no MFA & password vulnerabilities

955 accounts with no MFA & password vulnerabilities

220 Average number of apps per company

15 Average number of identities per employee

9% Identities have a weak, breached or reused password and no MFA

37% Identities are using passwords with no MFA

99% Identities are susceptible to phishing attacks (even with MFA)

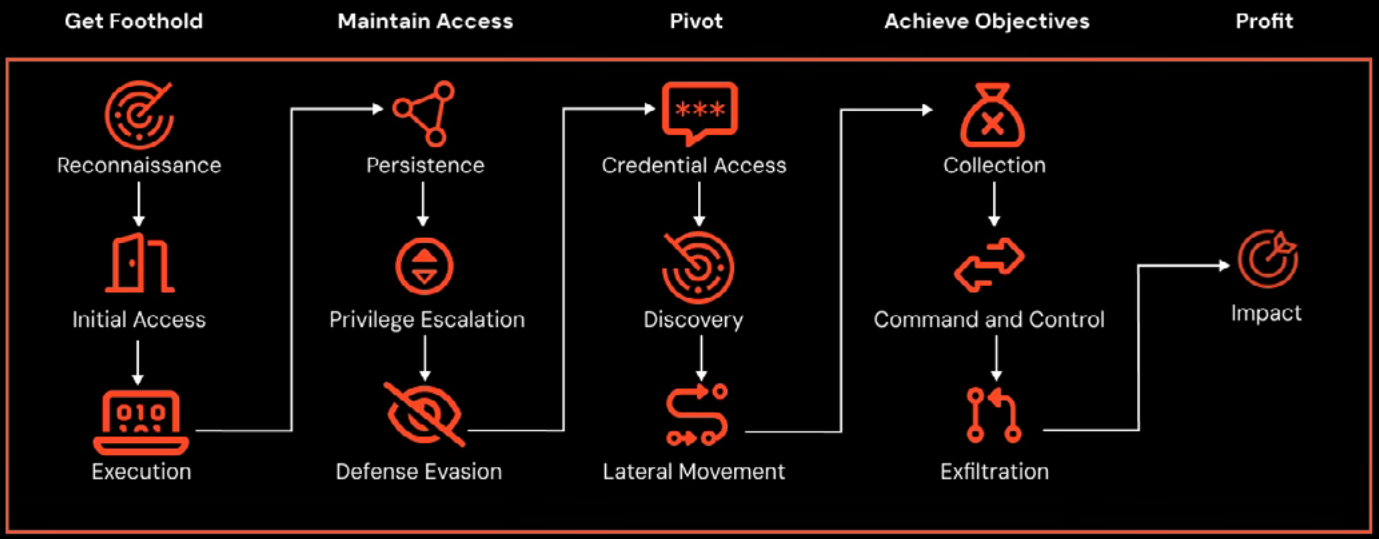
Attack paths are changing

Attackers can steal data within minutes, if not seconds of compromising a user account.

Unlike attacks against the network and endpoint, the window that security teams have to detect and respond to identity attacks once a user account is compromised is too narrow. There are little to no in-app protections, and almost no log data, to enable a security team to intercept the attacker before they achieve their goals. In nearly every case, by the time the security team responds to an identity breach, it's already too late.

Once they've gained access, the attacker will often simply dump the data from the app. To turn a profit, they sell the data to other criminals, or extort a ransom payment for the deletion of the data. From this point, attackers can then target other SaaS apps, cloud infrastructure, or on-premises assets to take more data and deploy ransomware to support their extortion efforts.

Network compromise in traditional environment



Get Foothold

Maintain Access

Pivot

Achieve Objectives

Profit

Reconnaissance

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

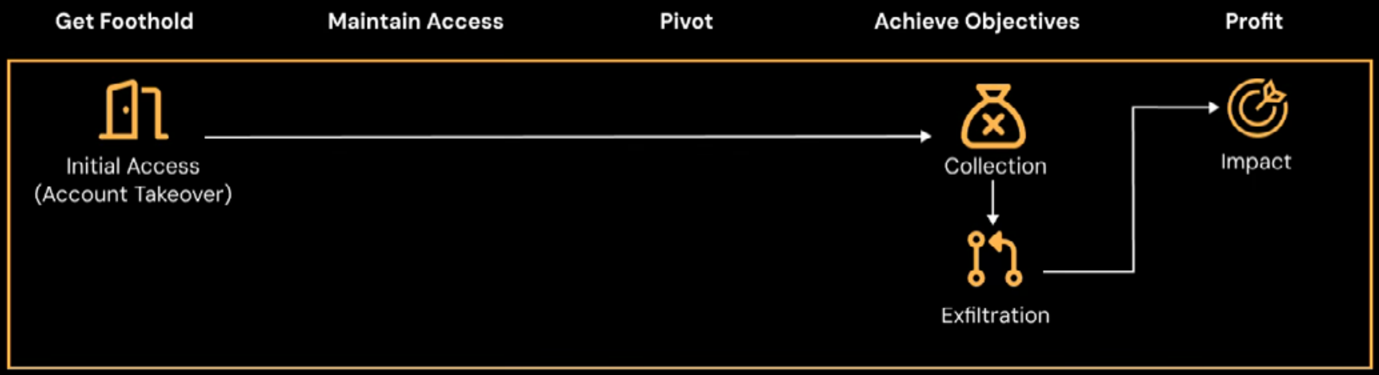
Collection

Command and Control

Exfiltration

Impact

Account takeover on third-party web app



Get Foothold

Maintain Access

Pivot

Achieve Objectives

Profit

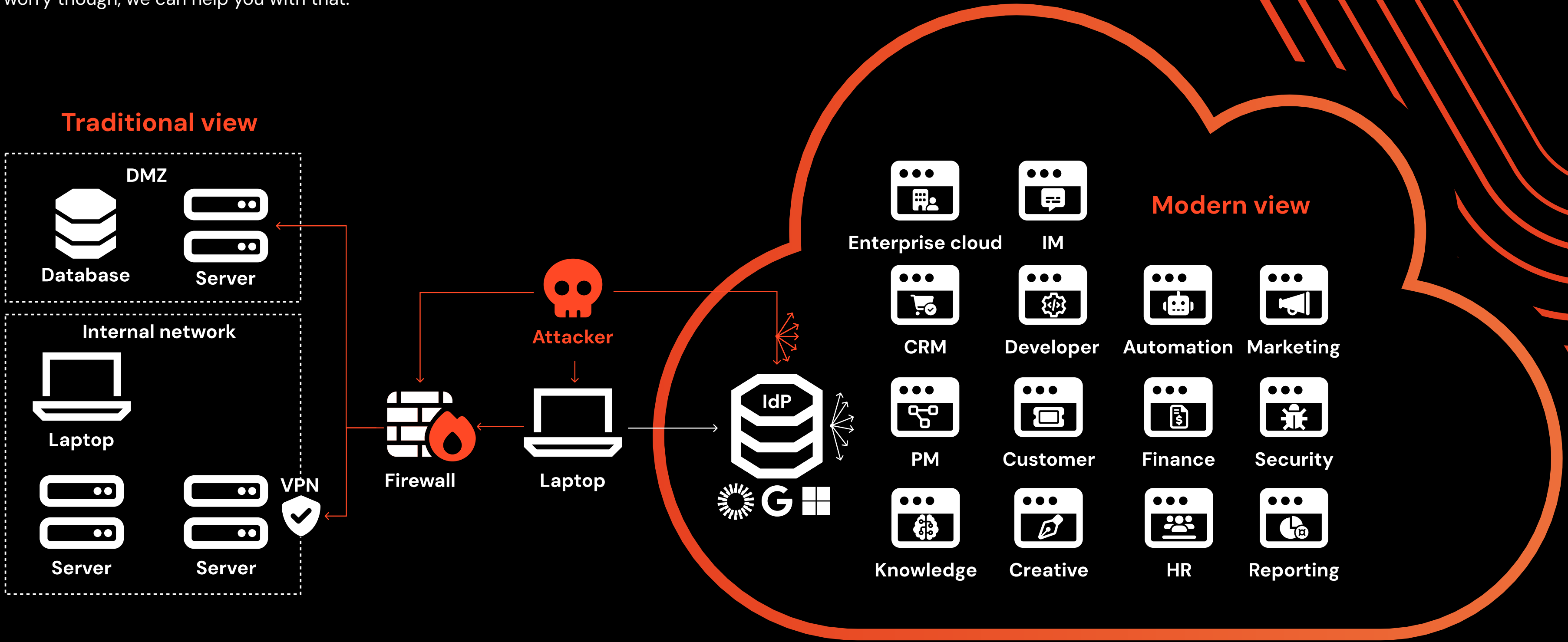
Initial Access
(Account Takeover)

Collection

Exfiltration

Impact

To combat the rise in identity attacks, a prevention-based approach is not enough — organizations need to both **proactively harden their attack surface and detect and stop identity attacks before their user accounts can be compromised.** To do this, a new telemetry source and control point is required — don't worry though, we can help you with that.



Push Security product overview

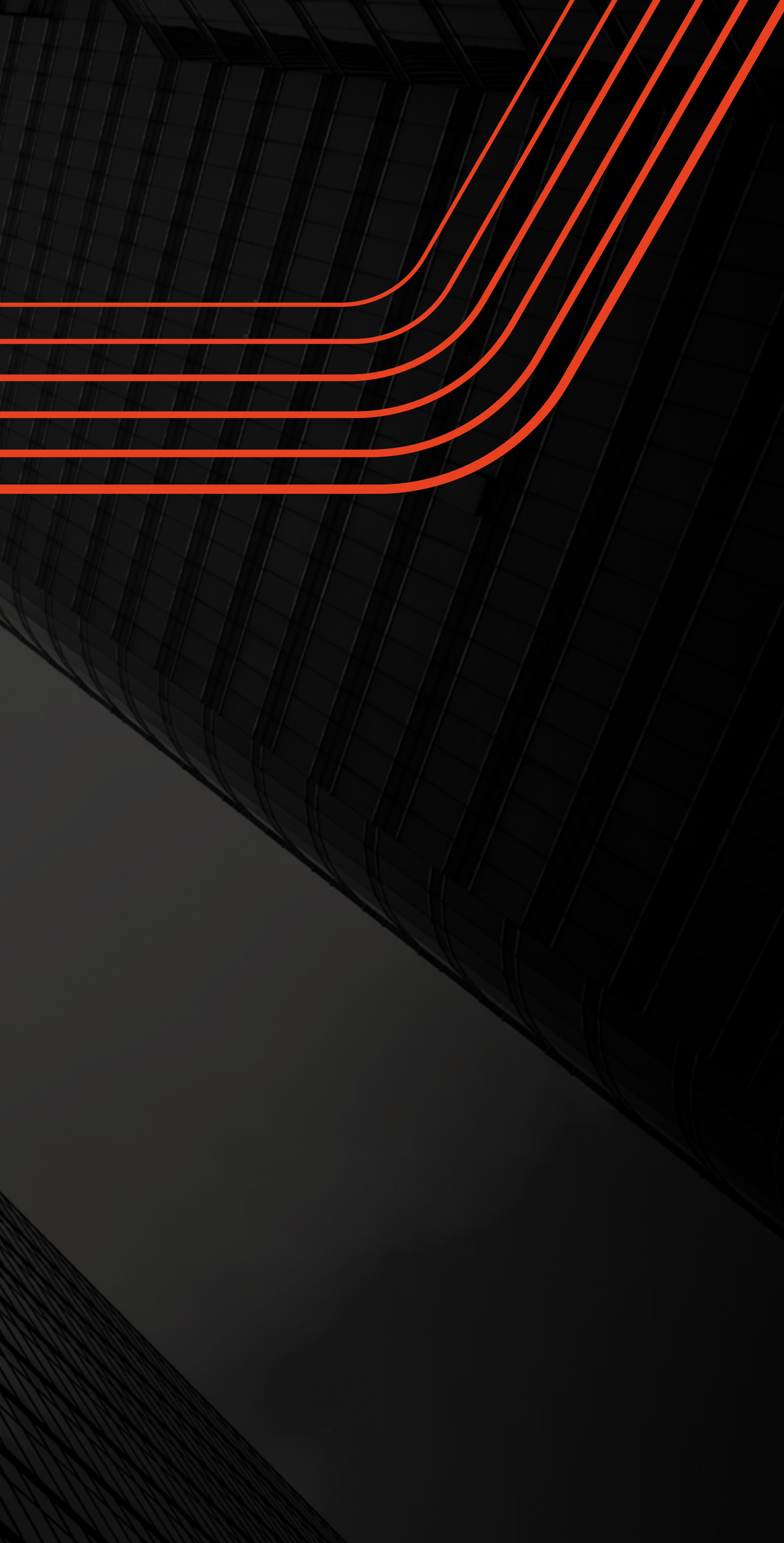
Push Security is the industry's first browser-native identity security platform. Push detects and stops identity attacks, prevents account takeover, and improves your overall identity security posture.

Think of Push as being like EDR, but in the browser. Using a browser extension, Push generates unique telemetry for detecting identity attacks in real time — e.g. phishing, credential stuffing, session hijacking — as well as surfacing exploitable identity vulnerabilities.

Upon making a detection, Push automatically enforces security controls directly in the browser to block attacks, fix vulnerabilities, and prevent risky user behaviors.

Security teams use Push to:

- **Map their full identity attack surface, including unmanaged identities on shadow apps.**
- **Detect identity attack TTPs that can't be observed using their existing threat monitoring tools.**
- **Uncover vulnerable and non-compliant user accounts outside of SSO, missing MFA and/or using stolen, leaked, weak and reused passwords.**
- **Secure corporate user accounts when verified credentials appear on criminal forums or in users' personal password managers.**
- **Proactively enforce controls in the browser such as MFA, SSO, strong & unique passwords and app-specific policies.**



Why the browser?

Push uses a browser extension like EDR uses an endpoint agent. It turns every employees' browser into a telemetry source and a control point for preventing, detecting and responding to identity attacks.

The browser is the gateway to the apps that your employees use to do their jobs every day. This is where the data and functionality now lives — and that attackers want. How do they access those apps? Via web identities.

The browser is the natural ingress point for identity data. It's the place where identities are created and used by employees — and also where attackers target them. So naturally, the best place to monitor and defend your identities is in the browser.

Being in the browser provides Push customers with rich telemetry on how identities are created, configured, and used, as well as providing a control point to detect, intercept, and shut down identity attacks as they happen in real time.

The Push browser agent provides a lightweight, low-compute solution that meets employees where they're at — in the browsers they are already using, with no changes to how or where they work.

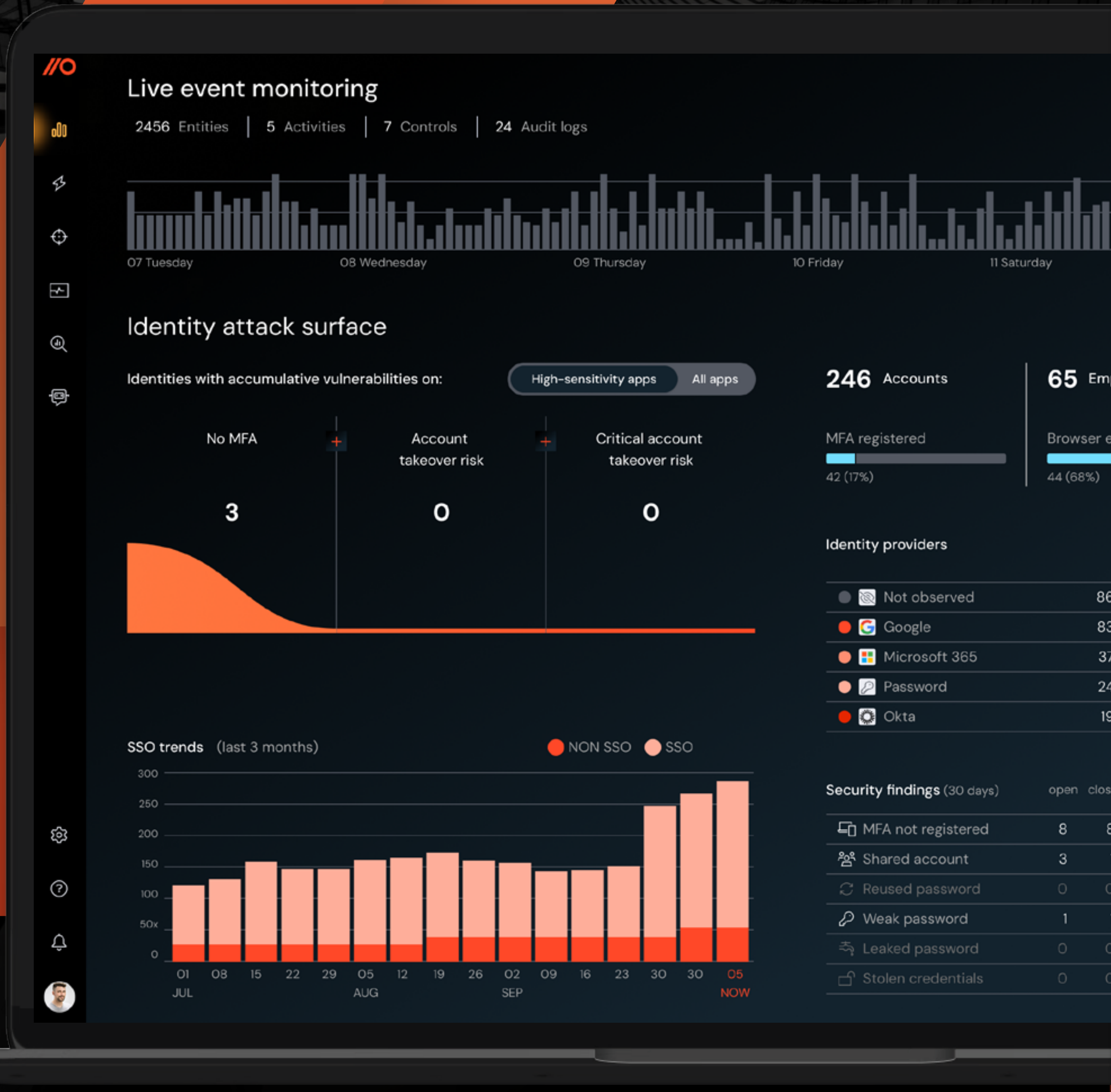
Push's lightweight browser extension can be deployed in minutes. Recently, Push Security deployed to 100,000 users in less than an hour on a regular business day, during normal office hours.

How Push works

Push is a SaaS platform that collects data through its browser extension and via a direct integration with enterprise IdPs (Okta, Microsoft, Google).

The Push browser extension collects identity data by observing employee browser activity, and then feeds that data into the Push platform for analysis and action. Users can consume the data through the admin console, API, and webhooks.

Here's a breakdown of the process.



Live event monitoring

2456 Entities | 5 Activities | 7 Controls | 24 Audit logs

Identity attack surface

Identities with accumulative vulnerabilities on:

No MFA	Account takeover risk	Critical account takeover risk
3	0	0

246 Accounts

MFA registered 42 (17%)

65 Em

Browser e 44 (68%)

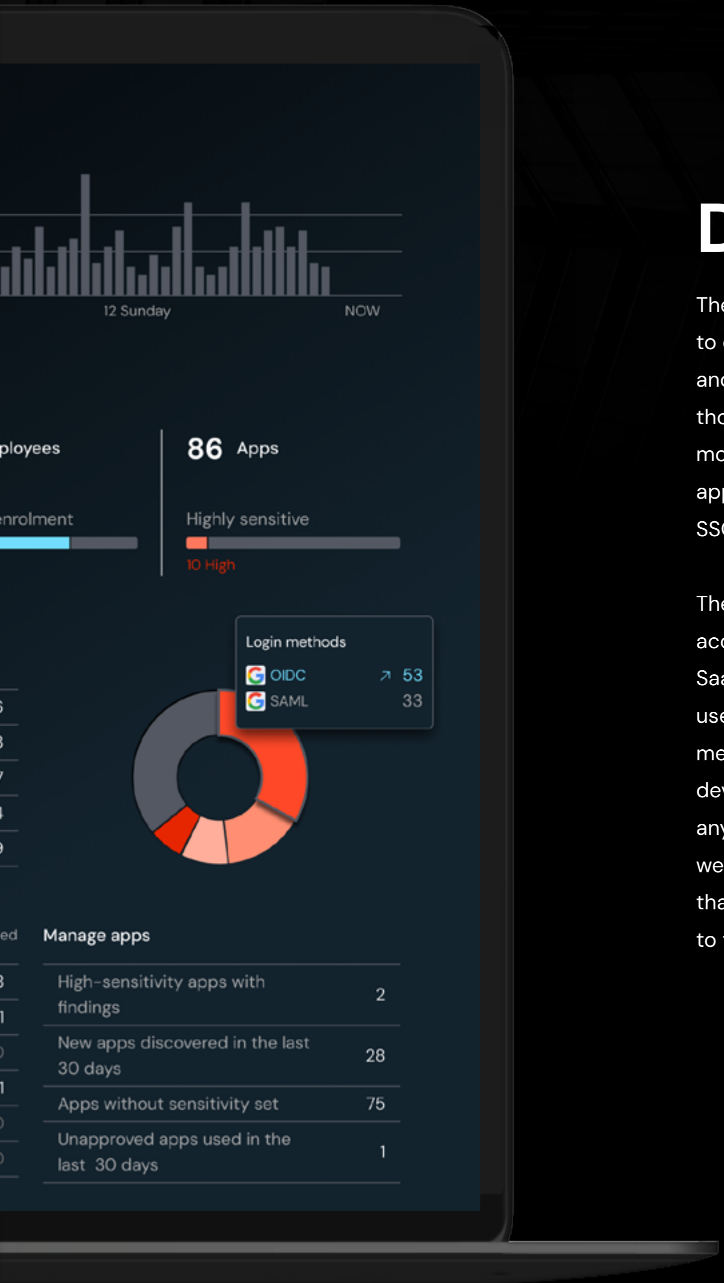
Identity providers

Not observed	86
Google	83
Microsoft 365	37
Password	24
Okta	19

SSO trends (last 3 months)

Security findings (30 days)

	open	clos
MFA not registered	8	8
Shared account	3	
Reused password	0	0
Weak password	1	
Leaked password	0	0
Stolen credentials	0	0



Manage apps

High-sensitivity apps with findings	2
New apps discovered in the last 30 days	28
Apps without sensitivity set	75
Unapproved apps used in the last 30 days	1

Deploy

The Push browser extension is deployed to employee browsers. It observes logins and signups to cloud accounts, whether those are federated or unfederated. It monitors how employees are accessing applications, including those not behind SSO.

The extension collects authentication and account data when employees log into SaaS applications, including the app URL, username, login method, MFA status and method, browser name and version, and device OS. This includes information about any credentials used to be able to identify weak, breached, and reused passwords that make the account more susceptible to takeover attempts.

Push generates a shortened, salted SHA256 hash of the password called a “password fingerprint” and stores it locally, meaning the password never leaves the employee browser. Push then uses the fingerprint to perform various health checks and identify vulnerabilities.

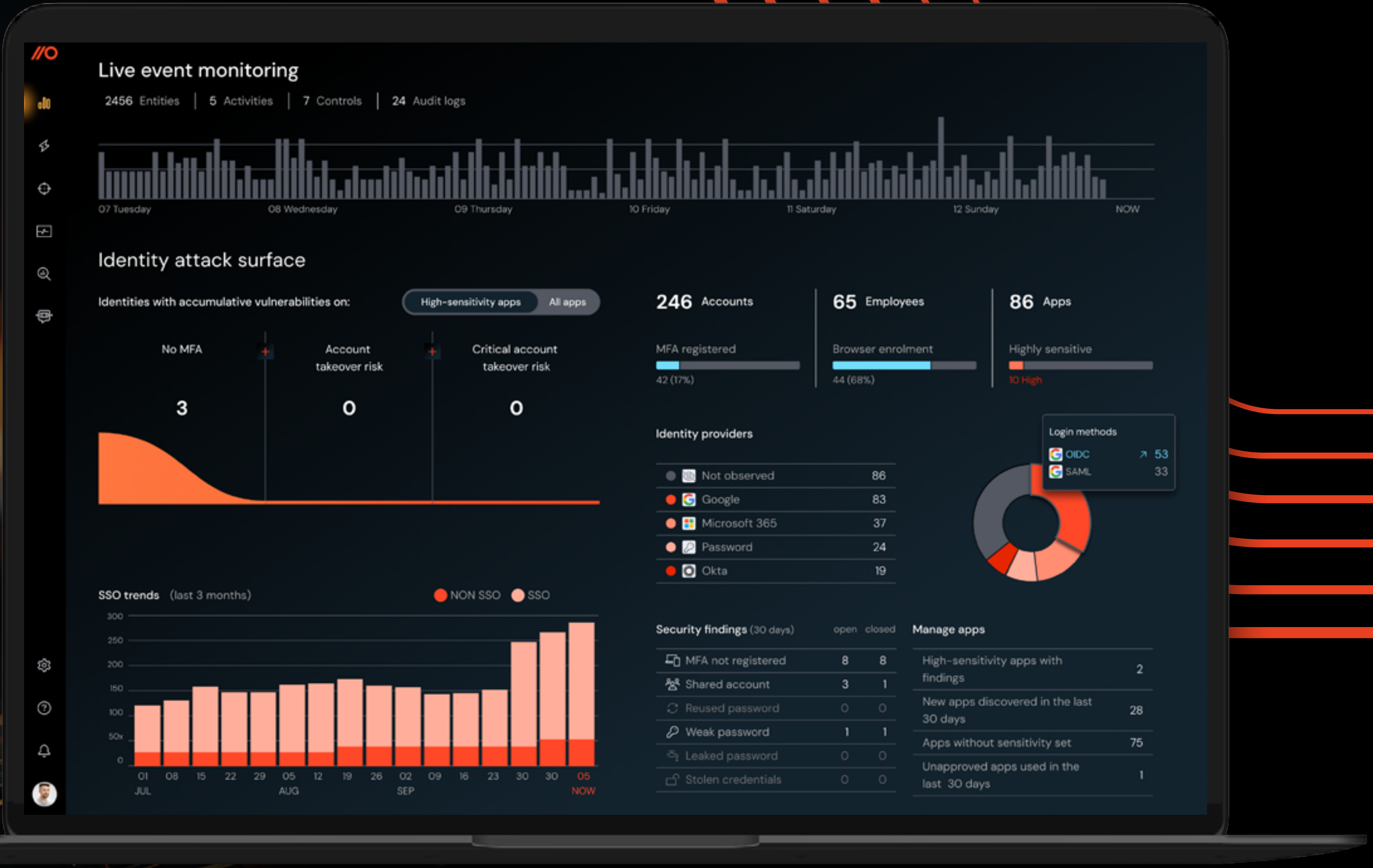
Push also integrates with your IdP via API to sync data on employees, SSO-supported apps, third-party OAuth integrations, and OIDC logins to further enrich the data collected in the browser.

Configure

Administrators can configure and manage Push through an admin console. The admin console provides a dashboard for reporting, as well as detailed data tables for all apps, accounts, and employees, and their associated security findings.

Using the admin console, customers can configure a range of features and controls that respond to the data collected by the browser extension. This enables Push customers to detect and respond to common identity attack techniques, with real-time interception of threats as the employee works in their browser. (More on these capabilities later.)

Push's controls generate events that can be used for threat detection, security investigations, and incident response, displayed in a real-time events feed.



Live event monitoring

2456 Entities | 5 Activities | 7 Controls | 24 Audit logs

Identity attack surface

Identities with accumulative vulnerabilities on: High-sensitivity apps | All apps

No MFA	Account takeover risk	Critical account takeover risk
3	0	0

246 Accounts
MFA registered
42 (17%)

65 Employees
Browser enrolment
44 (68%)

86 Apps
Highly sensitive
10 High

Identity providers

● Not observed	86
● Google	83
● Microsoft 365	37
● Password	24
● Okta	19

Login methods

OIDC	↗ 53
SAML	33

Security findings (30 days)	open	closed
MFA not registered	8	8
Shared account	3	1
Reused password	0	0
Weak password	1	1
Leaked password	0	0
Stolen credentials	0	0

Manage apps	
High-sensitivity apps with findings	2
New apps discovered in the last 30 days	28
Apps without sensitivity set	75
Unapproved apps used in the last 30 days	1

Integrate

Push provides a REST API and webhooks so that customers can send data to other security tools. This allows integration with SIEM, XDR, SOAR, compliance platforms, logging stacks, and more.

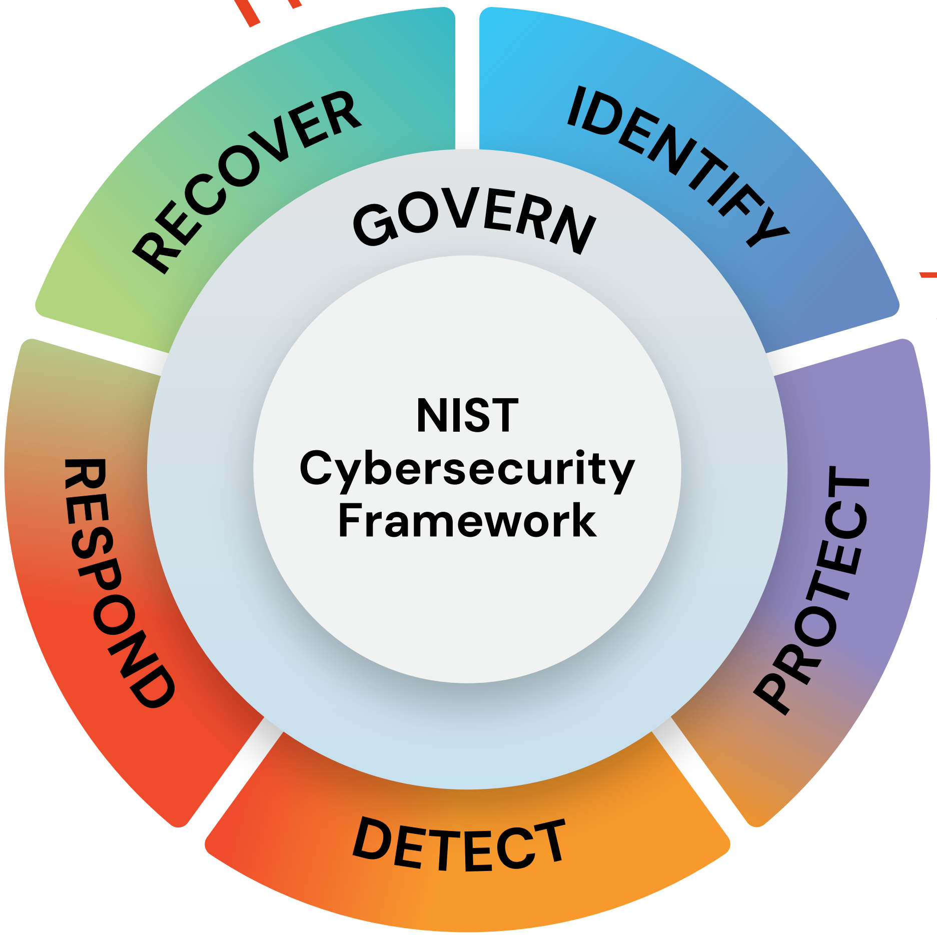
Webhooks can be set up to send security events to monitoring and logging tools in response to Push’s security controls being triggered, or high-risk vulnerabilities being discovered.

Push telemetry provides rich context for incident investigation and response, and correlation with other log sources to give blue teams a complete picture of an event so they can respond faster and with greater confidence.

How Push stops identity attacks and secures your identity attack surface

Push gives security teams the tools to implement an identity-first security strategy, providing a comprehensive ITDR capability for mapping, protecting and defending their entire identity attack surface and SaaS environment.

It's useful to apply common security models such as the 6 functions of the NIST Cybersecurity Framework to map the outcomes that Push delivers.



Push provides comprehensive identity security capabilities delivering key outcomes across all NIST cybersecurity functions.

NIST Function	Push Outcomes
Identify	Discover all workforce identities, apps, accounts, authentication methods, MFA coverage, and OAuth integrations to profile your attack surface.
Protect	Harden your identity attack surface by addressing MFA gaps, compromised / weak passwords, and non-SSO (ghost) logins.
Detect	Detect and block identity attacks like phishing, compromised credentials, and session theft.
Respond	Automatically execute response actions in real-time to block attacks and provide data to support incident investigations and response.
Recover	Deploy countermeasures and remediations to secure vulnerable identities and prevent corporate accounts and tenants from being compromised.
Govern	Enforce policies, deploy controls, and report key metrics for compliance (e.g. accurate SSO and MFA coverage, identity hygiene, third-party risk management).

Scan to book a demo

Identify

Discover all workforce identities, apps, accounts, authentication methods, MFA coverage, and OAuth integrations to profile your attack surface.

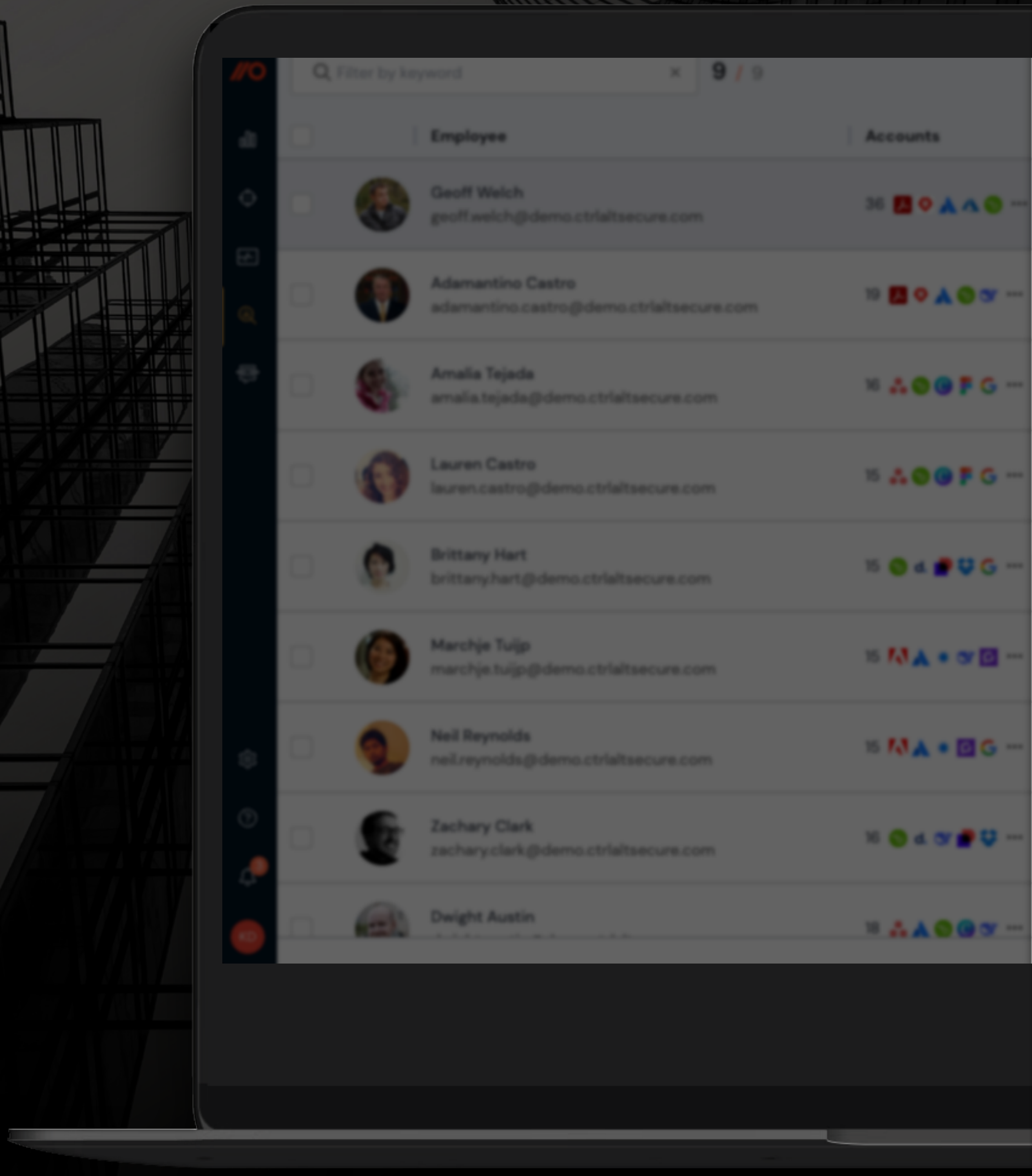
The browser extension observes all login types and authentication methods as they are used in your employee's browser, identifying:

- Whether employees are registered for MFA; which MFA methods they are using; and which accounts are missing MFA.

- Third-party OAuth integrations connected to your workspace and the permissions granted.

- The apps being used throughout your organization, showing user activity, access methods, and potential security risks.

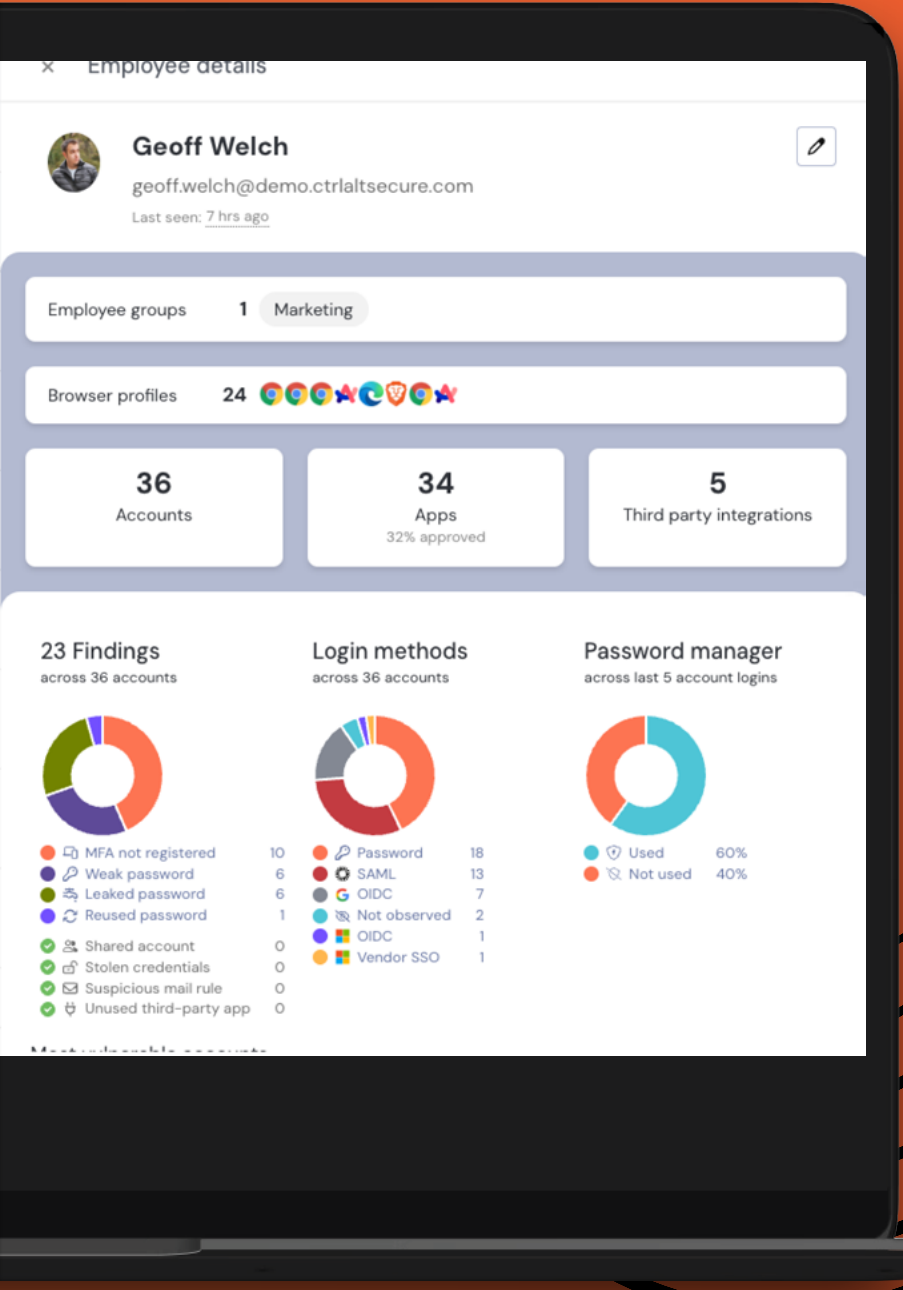
- Where credentials are being stored in password managers, and which password managers are being used.



Filter by keyword ✕ 9 / 9

Employee	Accounts
Geoff Welch geoff.welch@demo.ctrlaltsecure.com	36
Adamantino Castro adamantino.castro@demo.ctrlaltsecure.com	19
Amalia Tejada amalia.tejada@demo.ctrlaltsecure.com	16
Lauren Castro lauren.castro@demo.ctrlaltsecure.com	15
Brittany Hart brittany.hart@demo.ctrlaltsecure.com	15
Marchje Tuijp marchje.tuijp@demo.ctrlaltsecure.com	15
Neil Reynolds neil.reynolds@demo.ctrlaltsecure.com	15
Zachary Clark zachary.clark@demo.ctrlaltsecure.com	16
Dwight Austin	18

Push then displays high-level trends in a dashboard to highlight vulnerable and non-compliant identities and apps. Information can be sorted and analyzed by app, employee, account, and browser.



× Employee details

Geoff Welch
geoff.welch@demo.ctrlaltsecure.com
Last seen: 7 hrs ago

Employee groups	1	Marketing
Browser profiles	24	

36	34	5
Accounts	Apps 32% approved	Third party integrations

23 Findings
across 36 accounts

●	MFA not registered	10
●	Weak password	6
●	Leaked password	6
●	Reused password	1
✓	Shared account	0
✓	Stolen credentials	0
✓	Suspicious mail rule	0
✓	Unused third-party app	0

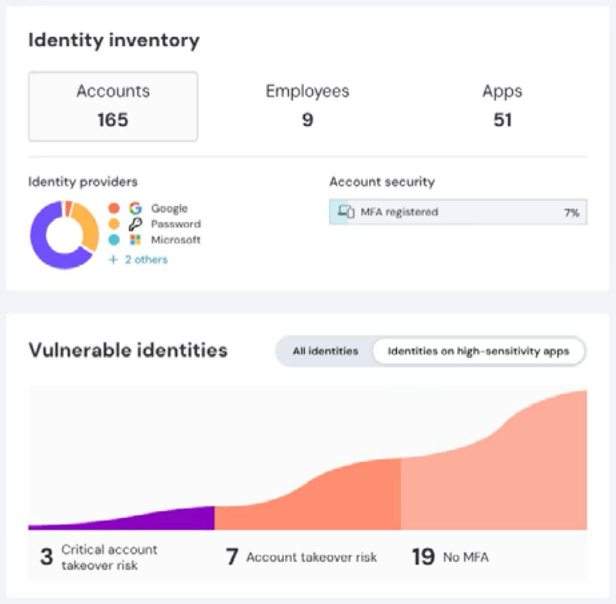
Login methods
across 36 accounts

●	Password	18
●	SAML	13
●	OIDC	7
●	Not observed	2
●	OIDC	1
●	Vendor SSO	1

Password manager
across last 5 account logins

●	Used	60%
●	Not used	40%

Most vulnerable accounts



Identity inventory

Accounts	Employees	Apps
165	9	51

Identity providers
● Google
● Password
● Microsoft
+ 2 others

Account security
MFA registered 7%

Vulnerable identities

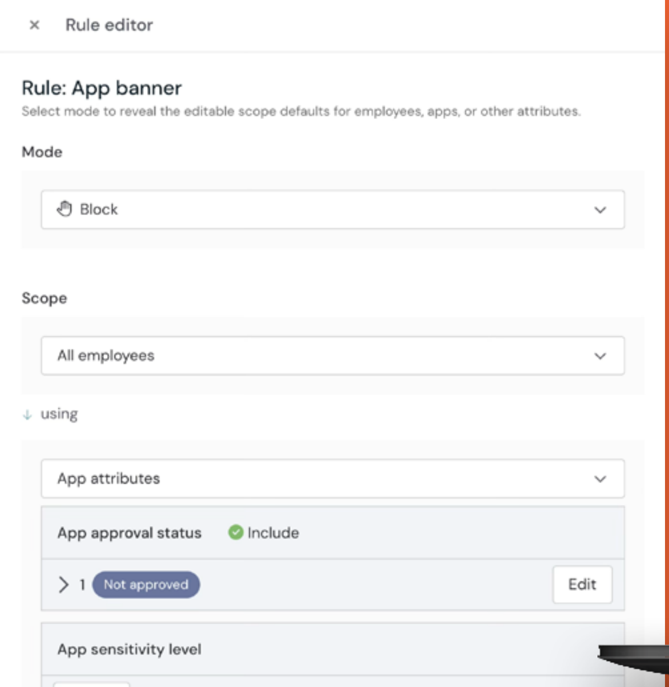
3	Critical account takeover risk
7	Account takeover risk
19	No MFA

Protect

Harden your identity attack surface by addressing MFA gaps, compromised / weak passwords, and non-SSO (ghost) logins.

Using the data gathered when mapping the identity attack surface, Push then hardens it by enforcing security controls at the point of login in the browser. Push reduces your attack surface by blocking access to unapproved apps and preventing the creation of local accounts.

Fully configurable app banners guide your employees to use approved apps and secure logins, instruct on safe app use at the point of access, and outright block apps that are not authorized for company use.



× Rule editor

Rule: App banner

Select mode to reveal the editable scope defaults for employees, apps, or other attributes.

Mode: Block

Scope: All employees

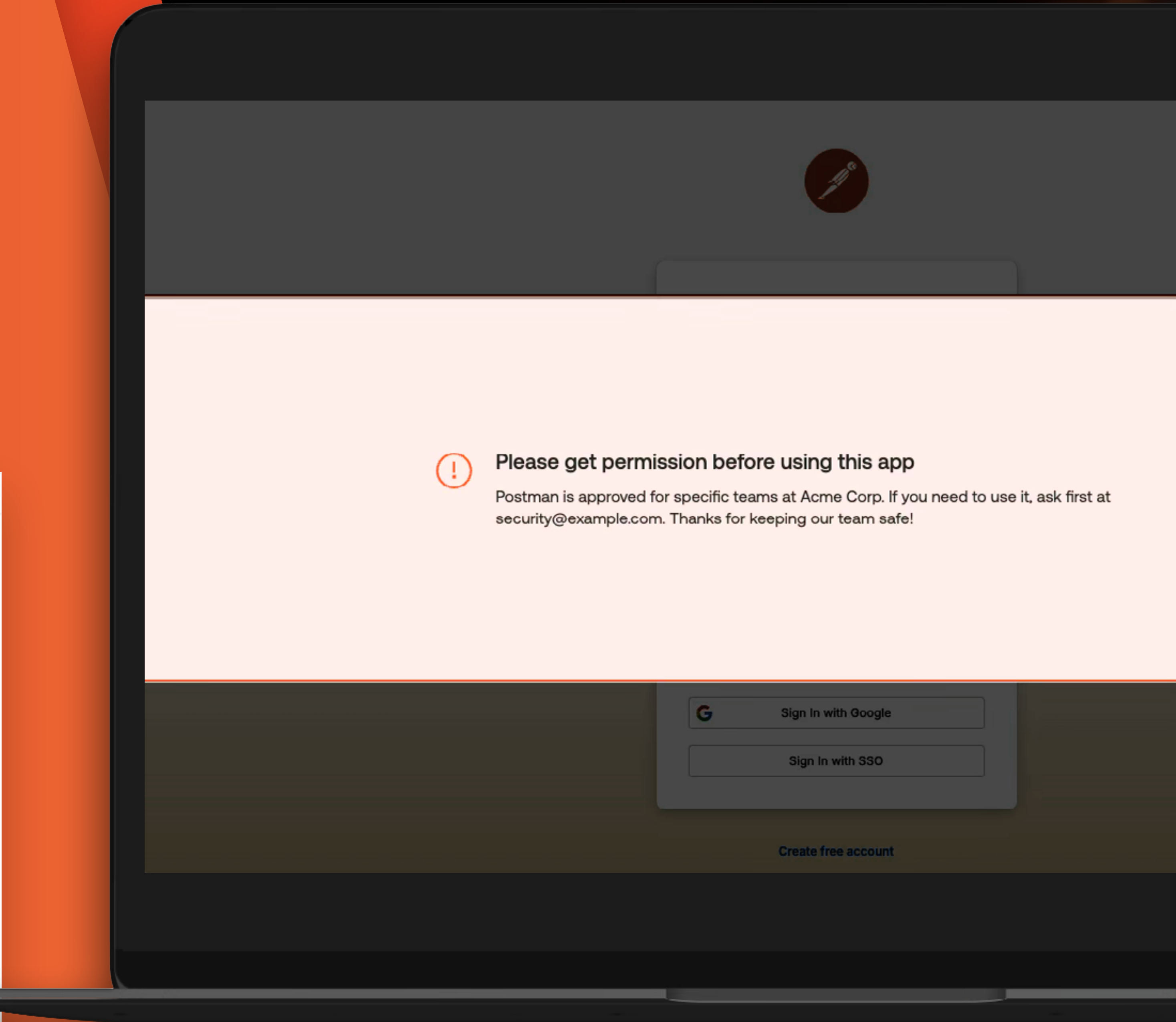
↓ using

App attributes

App approval status ✓ Include

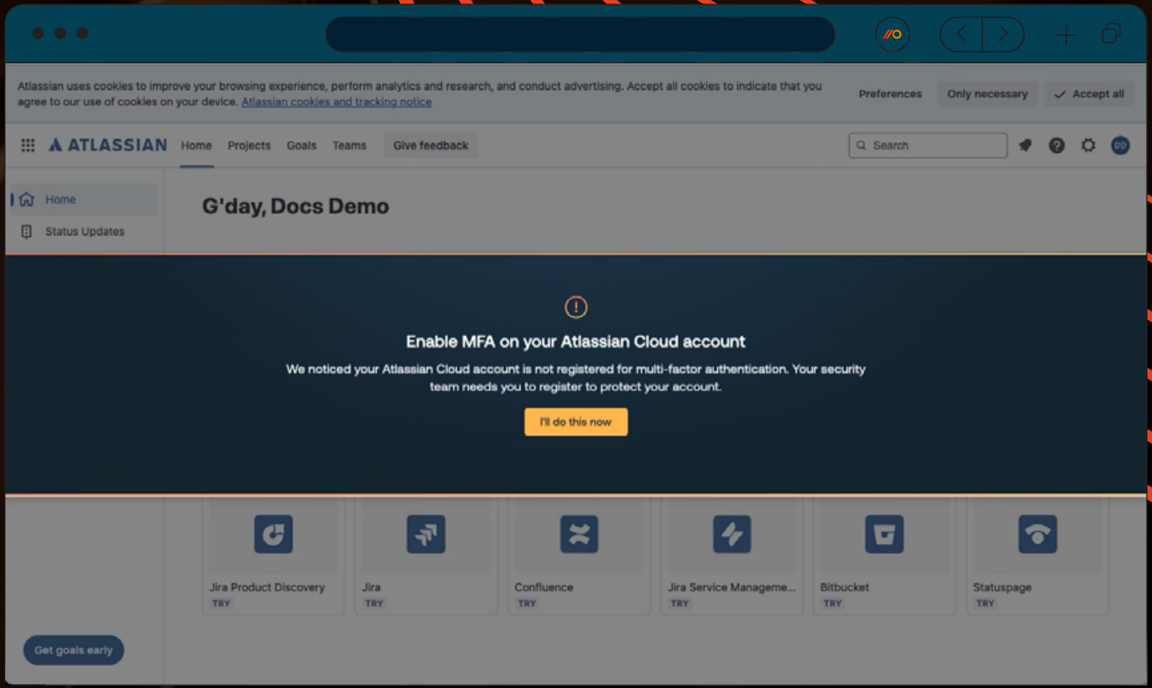
› 1 Not approved — Edit

App sensitivity level



Please get permission before using this app

Postman is approved for specific teams at Acme Corp. If you need to use it, ask first at security@example.com. Thanks for keeping our team safe!



Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising. Accept all cookies to indicate that you agree to our use of cookies on your device. Atlassian cookies and tracking notice

G'day, Docs Demo

Enable MFA on your Atlassian Cloud account

We noticed your Atlassian Cloud account is not registered for multi-factor authentication. Your security team needs you to register to protect your account.

Push can enforce MFA on employee accounts (even on unmanaged apps and when the app does not natively support it) prompting employees to enroll in MFA whenever it is missing at the point of login.

Push helps get more apps and accounts behind SSO, and can enforce SSO logins or block apps without SSO support.

It also encourages the use of sanctioned alternatives that are behind SSO.

Admins can configure the SSO password protection control to pin employee IdP credentials, preventing them from entering their IdP password into any other site, blocking phishing attempts and unsafe reuse of high-risk credentials.

Push also monitors for weak, breached, and reused passwords across the application landscape and can prompt users to change vulnerable passwords at login.

Detect

Detect and block identity attacks like phishing, compromised credentials, and session theft.

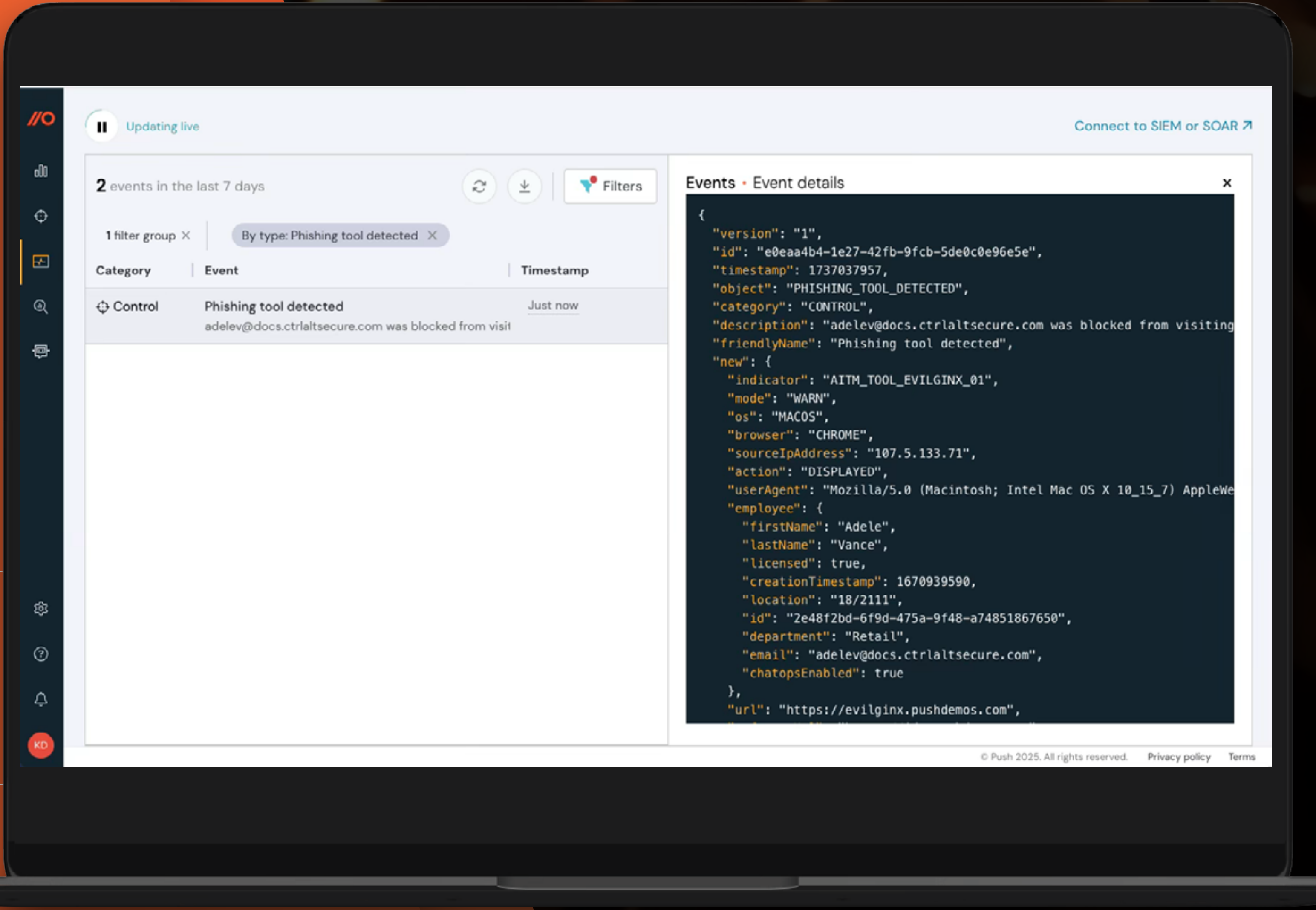
Push detects and blocks identity attacks in real-time by monitoring for malicious activity in employee browsers, as well as monitoring external sources for early notification of potential threats.

Push uses high-fidelity detections that target the TTPs used by attackers early in the attack chain that they cannot easily change or disguise — those high up the Pyramid of Pain. Because these detections are both high-fidelity and real-time, Push can use them to execute immediate response actions, using the browser as an enforcement point as well as a telemetry source.

These controls are designed to intercept attacker TTPs before account takeover occurs, rather than simply offering after-the-fact indicators of compromise post-breach.

Push detects phishing attacks by detecting malicious toolkits running on webpages including Adversary-in-the-Middle (AitM) and Browser-in-the-Middle (BitM) toolkits, and cloned login pages.

Because Push observes the DOM in real time, the typical obfuscation techniques used by attackers to disguise their malicious pages can be defeated. Learn more about how attackers are evading typical detection controls.



2 events in the last 7 days

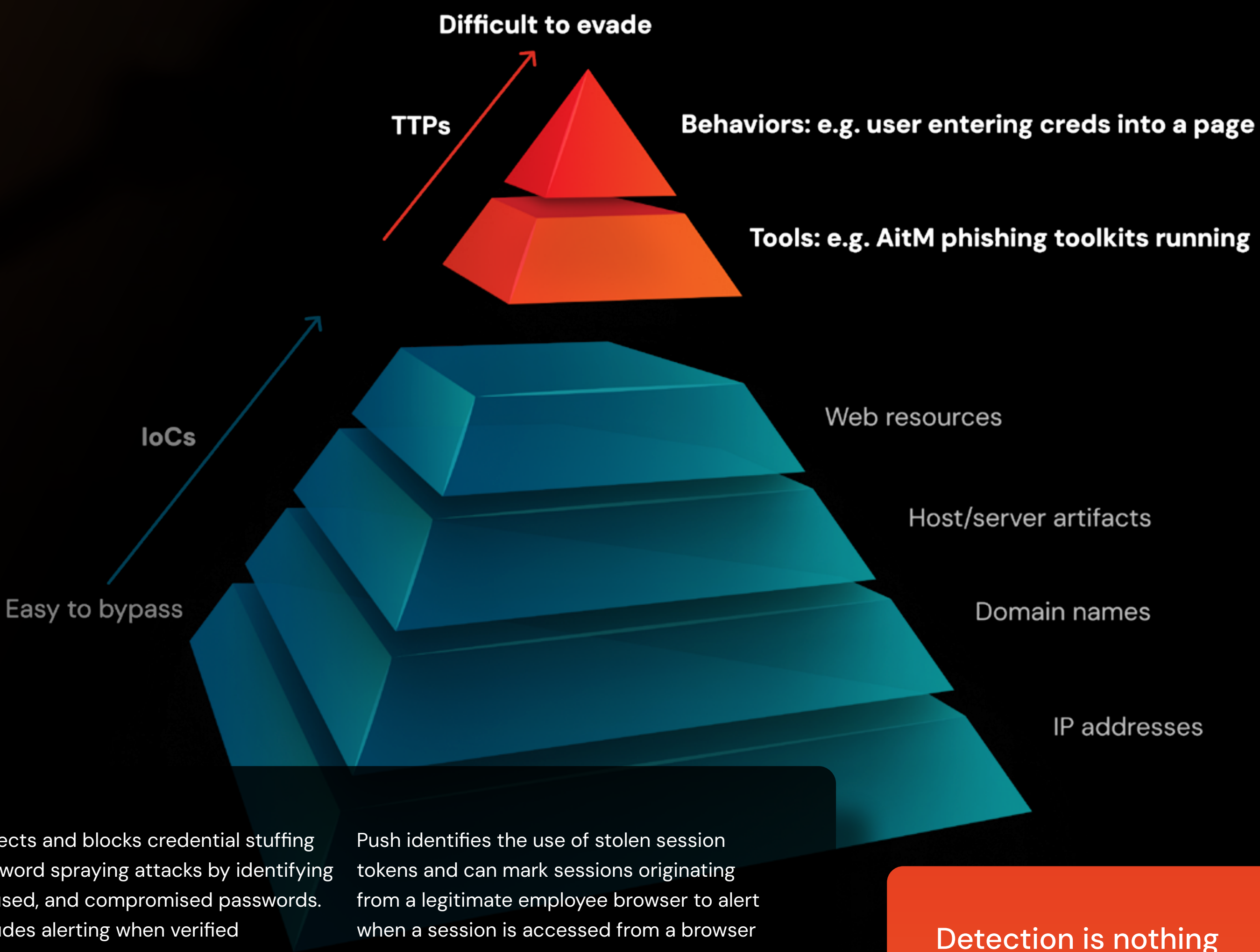
1 filter group ✕ By type: Phishing tool detected ✕

Category	Event	Timestamp
Control	Phishing tool detected adelev@docs.ctrlaltsecure.com was blocked from visit	Just now

Events • Event details ✕

```
{
  "version": "1",
  "id": "e0eaa4b4-1e27-42fb-9fcb-5de0c0e96e5e",
  "timestamp": 1737037957,
  "object": "PHISHING_TOOL_DETECTED",
  "category": "CONTROL",
  "description": "adelev@docs.ctrlaltsecure.com was blocked from visiting
  "friendlyName": "Phishing tool detected",
  "new": {
    "indicator": "AITM_TOOL_EVILGINX_01",
    "mode": "WARN",
    "os": "MACOS",
    "browser": "CHROME",
    "sourceIpAddress": "107.5.133.71",
    "action": "DISPLAYED",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWe
    "employee": {
      "firstName": "Adele",
      "lastName": "Vance",
      "licensed": true,
      "creationTimestamp": 1670939590,
      "location": "18/2111",
      "id": "2e48f2bd-6f9d-475a-9f48-a74851867650",
      "department": "Retail",
      "email": "adelev@docs.ctrlaltsecure.com",
      "chatopsEnabled": true
    },
    "url": "https://evilginx.pushdemos.com",
```

© Push 2025. All rights reserved. Privacy policy Terms



Push detects and blocks credential stuffing and password spraying attacks by identifying weak, reused, and compromised passwords. This includes alerting when verified credentials belonging to employees appear on criminal marketplaces.

Push is uniquely positioned to do this by using its browser extension to compare data from compromised credential TI feeds against fingerprints of the actual credentials employees are using when a session is accessed from a browser.

Push identifies the use of stolen session tokens and can mark sessions originating from a legitimate employee browser to alert when a session is accessed from a browser without the Push extension running.

When an alert is triggered, it appears on the Events page in the Push admin console, and can be sent via webhook and API to be used in manual and automated response workflows, in response to specific events, or as part of an incident investigation.

Detection is nothing unless you can do something with the data, which is why our detection controls also come with integrated response and remediation functionality.

Respond

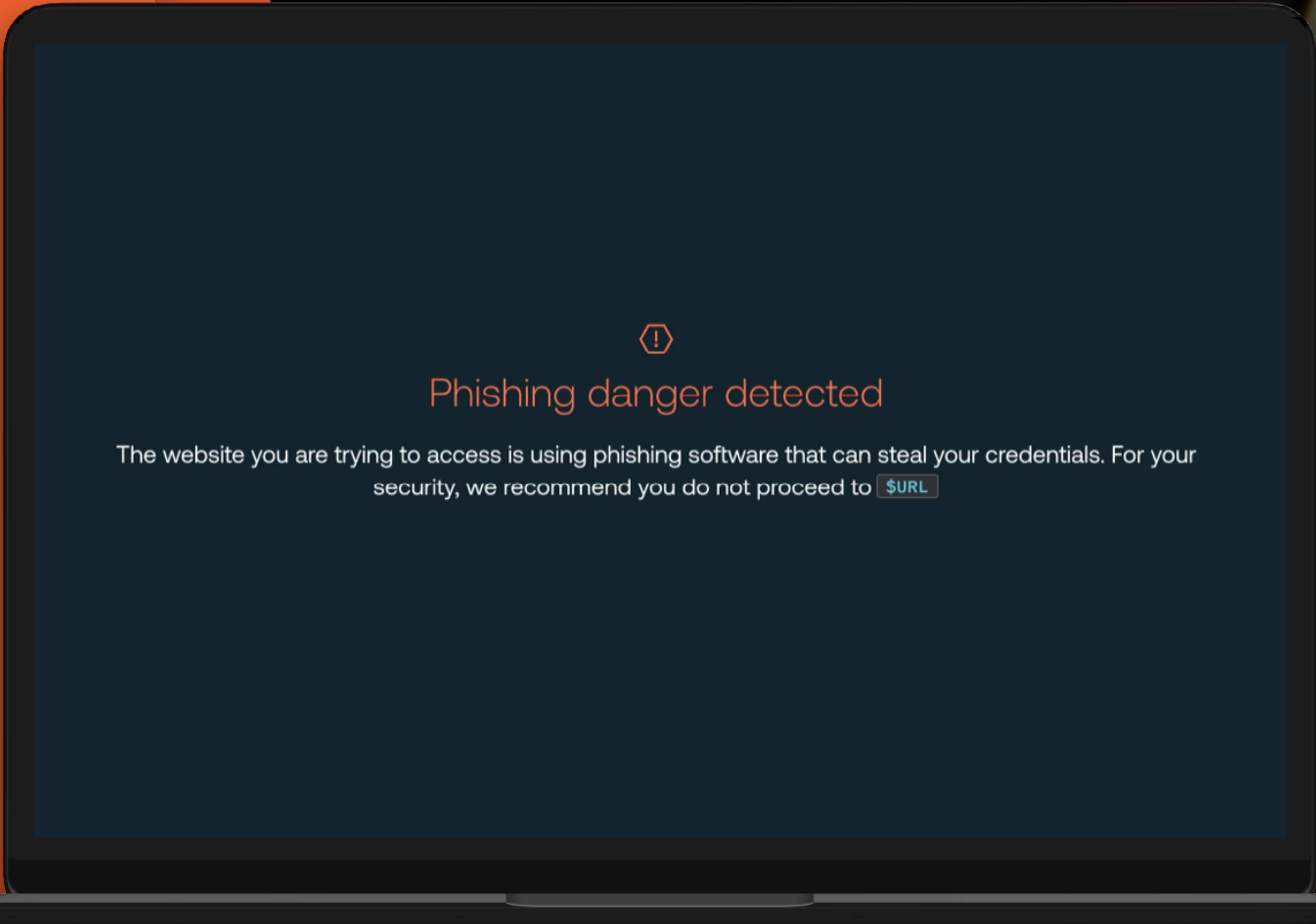
Automatically execute response actions in real-time to block attacks and provide data to support incident investigations and response.

The high-fidelity and real time nature of the detections developed by Push enables automated and immediate response actions to also be executed in the browser. These block attacks and risky user behaviors.

For example, when a phishing toolkit or cloned login page is detected, the user will be prevented from interacting with the page, and Push will display a customized message in the form of a full-page screen.

When a user attempts to enter their SSO password into a phishing site (either typed, copied from a password manager or other external source, or autofilled) the action will be intercepted before the credentials are submitted, blocking the phishing attempt.

Once malicious sites are detected, they can be added to blocklists to prevent them being accessed by employees.



Phishing danger detected

The website you are trying to access is using phishing software that can steal your credentials. For your security, we recommend you do not proceed to $URL

Incident responders can leverage the Push API to quickly interrogate attack surface data and respond to limit the blast radius of a compromise.

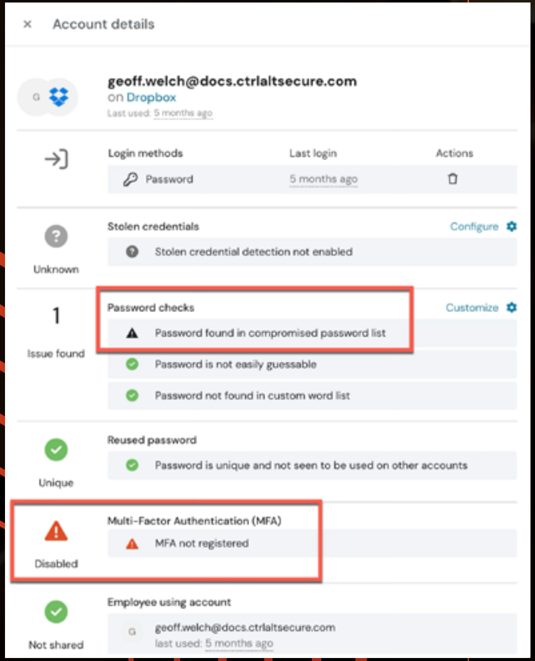
For example:

- When a stolen credential is detected, Push shows whether the account has MFA, and whether the password was used on other accounts.

- If a third-party app is subject to a data breach or ongoing malicious campaign, security teams can deploy app banners to manage or block its use, and prompt users to urgently configure MFA the next time it is accessed.

- Where an account takeover is suspected, Push can identify any risky OAuth integrations or where credentials are reused elsewhere to quickly deploy mitigations on further accounts with potential vulnerabilities, e.g. changing passwords, configuring strong MFA, etc.

Responders can also leverage Push data to address identity vulnerabilities and control gaps.



× Account details

geoff.welch@docs.ctrlaltsecure.com
on Dropbox
Last used: 5 months ago

Login methods	Last login	Actions
Password	5 months ago	🗑

Stolen credentials — Configure
? Stolen credential detection not enabled
Unknown

Password checks — Customize
1 Issue found
▲ Password found in compromised password list
✓ Password is not easily guessable
✓ Password not found in custom word list

Reused password
✓ Password is unique and not seen to be used on other accounts
Unique

Multi-Factor Authentication (MFA)
▲ MFA not registered
Disabled

Employee using account
geoff.welch@docs.ctrlaltsecure.com
last used: 5 months ago
Not shared

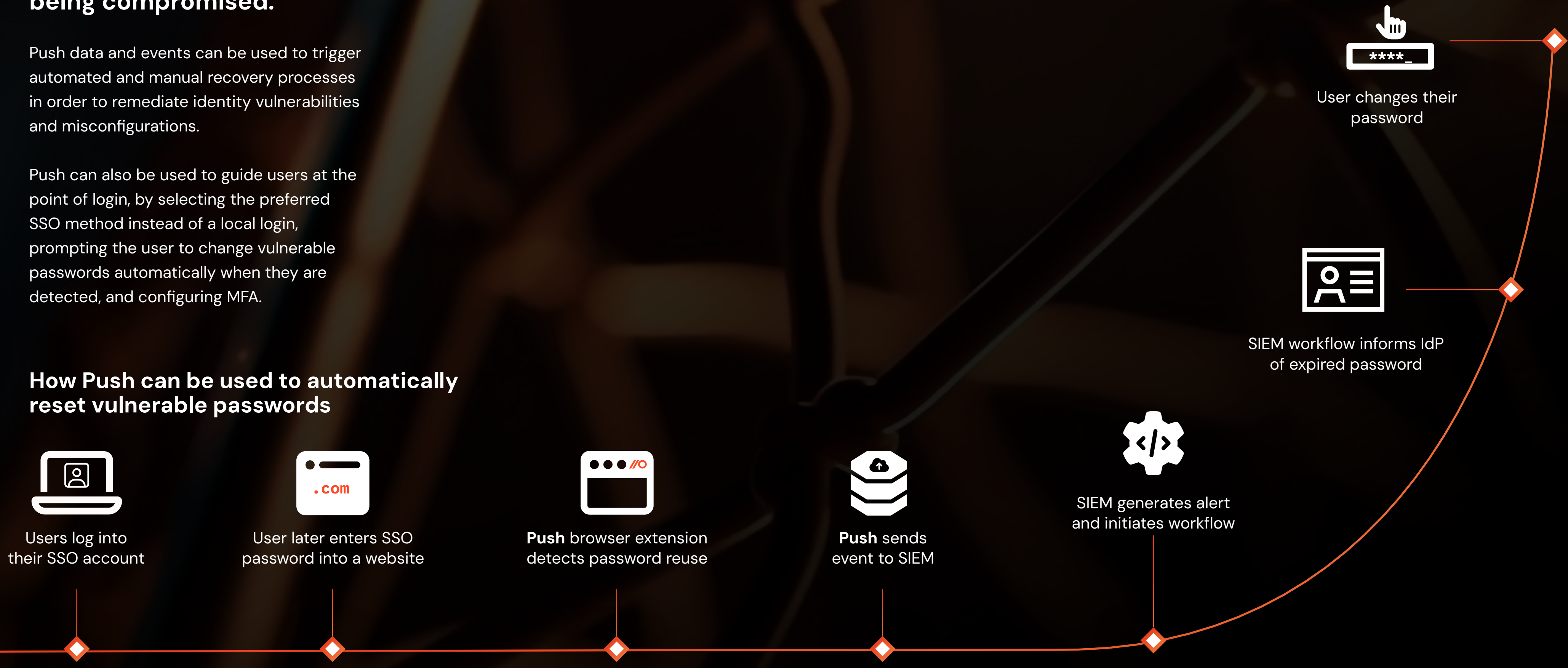
Recover

Deploy countermeasures and remediations to secure vulnerable identities and prevent corporate accounts and tenants from being compromised.

Push data and events can be used to trigger automated and manual recovery processes in order to remediate identity vulnerabilities and misconfigurations.

Push can also be used to guide users at the point of login, by selecting the preferred SSO method instead of a local login, prompting the user to change vulnerable passwords automatically when they are detected, and configuring MFA.

How Push can be used to automatically reset vulnerable passwords



Users log into their SSO account

User later enters SSO password into a website

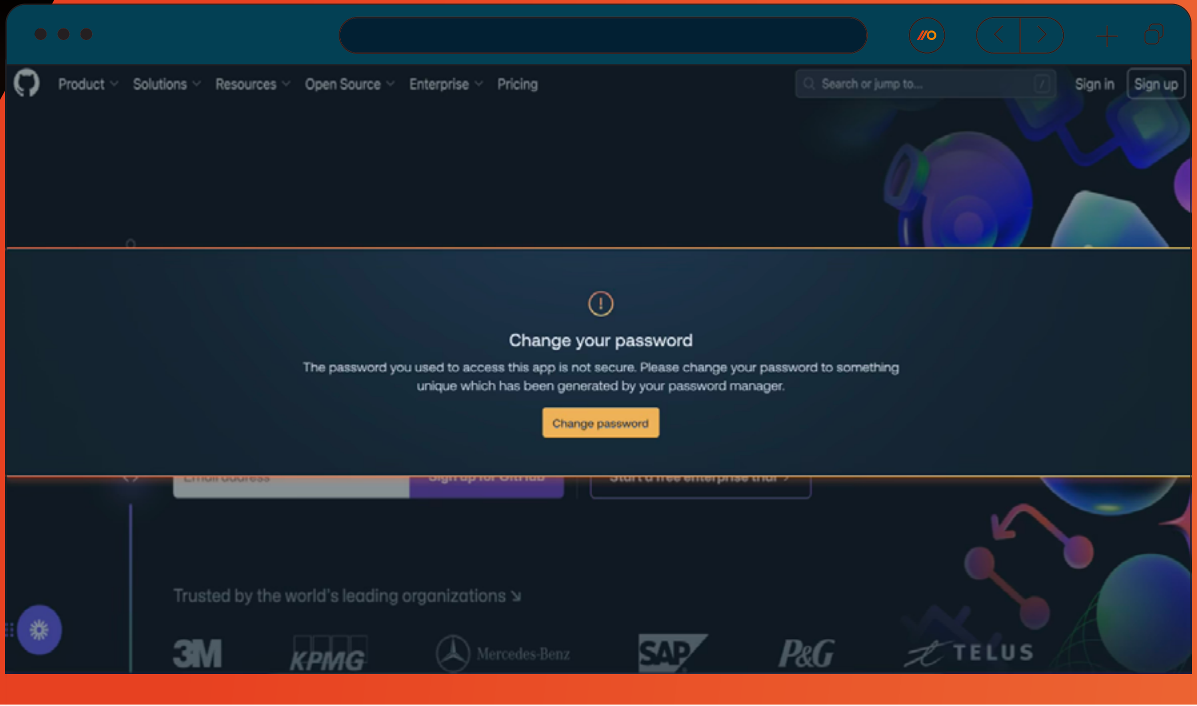
Push browser extension detects password reuse

Push sends event to SIEM

SIEM generates alert and initiates workflow

SIEM workflow informs IdP of expired password

User changes their password



Change your password

The password you used to access this app is not secure. Please change your password to something unique which has been generated by your password manager.

Change password

When a high-risk app or account is identified with MFA coverage gaps, Push can be used to prompt MFA registration whenever a user logs into the app.

Push's API and webhooks can also be used to monitor MFA coverage and trigger security alerts in your SIEM to facilitate manual follow-up where needed.

Push data can be used to inform broader recovery projects following an incident or near-miss, by initiating broader change projects across the attack surface, by for example:

- **Extending SSO coverage to additional work applications.**
- **Improving MFA coverage and removing phishable MFA factors.**
- **Removing risky OAuth integrations.**
- **Blocking high-risk apps and guiding users to approved alternatives.**
- **Identifying where corporate passwords are being stored in users' personal password managers**

Govern

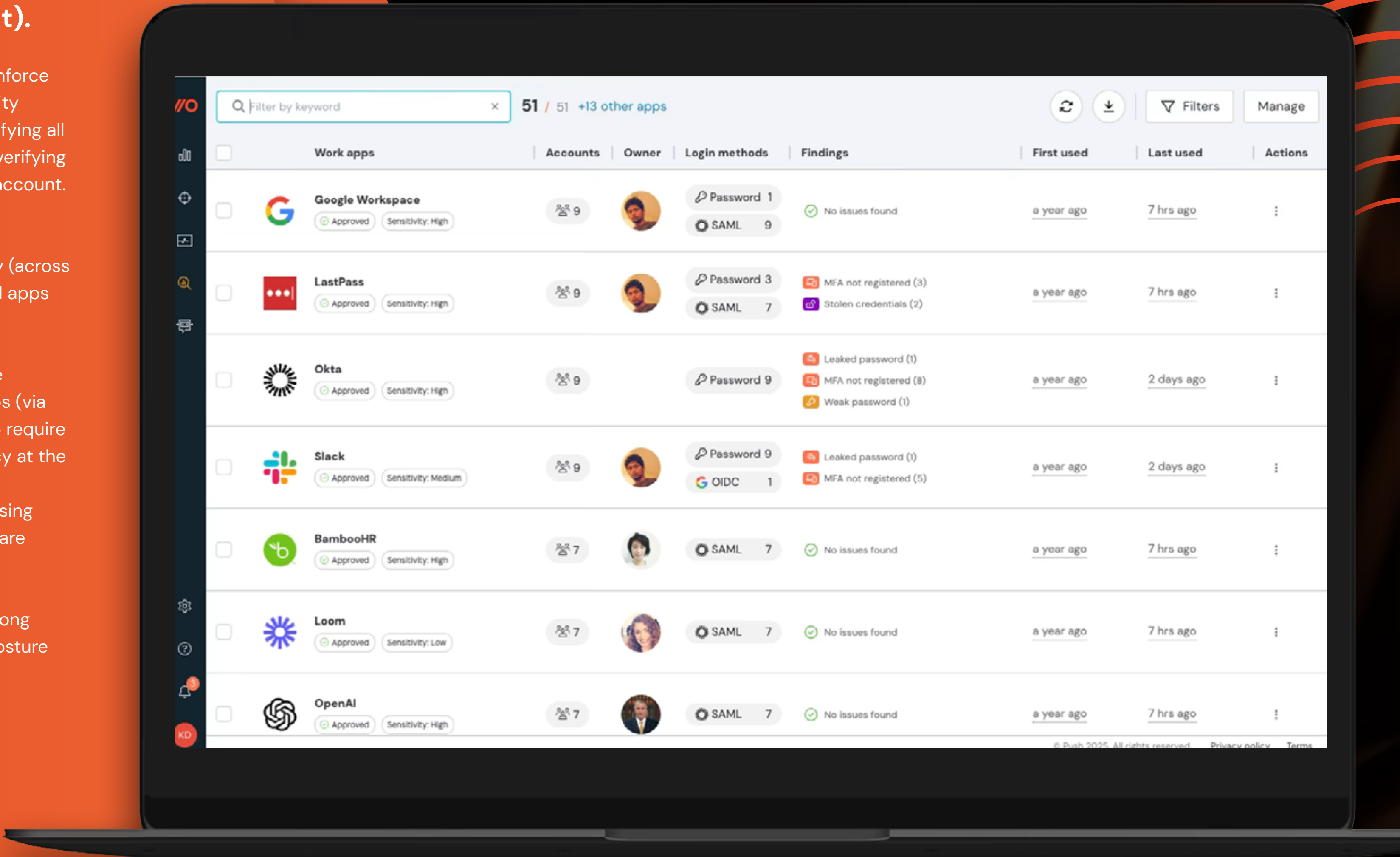
Enforce policies, deploy controls, and report key metrics for compliance (e.g. accurate SSO and MFA coverage, identity hygiene, third-party risk management).

Push enables you to measure, monitor, and enforce compliance across your entire app and identity surface, meeting security standards by identifying all the third-party services employees use and verifying the authentication controls protecting each account. Using Push, you can:

- Create and manage an application inventory (across internal and third-party apps), identifying all apps used by employees.

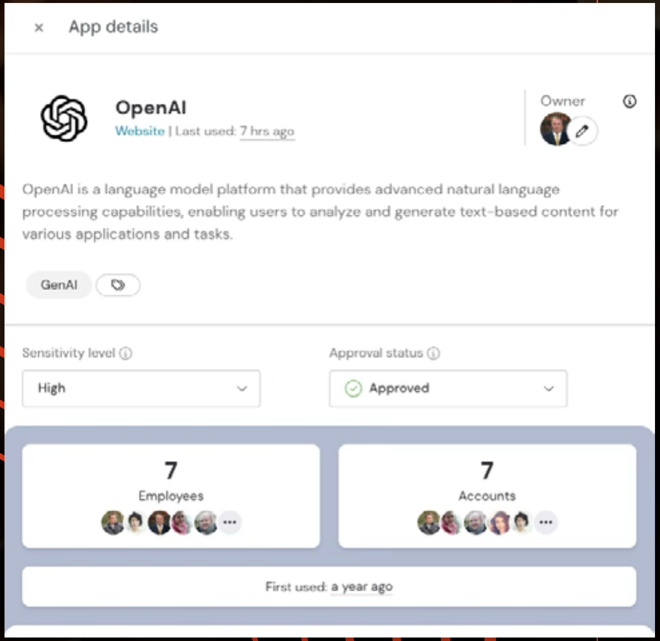
- Enforce security policies on every employee account, whether on centrally managed apps (via your enterprise IdP) or not. It can be used to require employee acknowledgment of security policy at the point of use (e.g. requiring employees to acknowledge usage guidelines before accessing GenAI tools), and these acknowledgements are logged and tracked for future reference.

- Enforce policies like mandatory MFA and strong passwords and provide accurate security posture reporting on a per-account basis.



☐	Work apps	Accounts	Owner	Login methods	Findings	First used	Last used	Actions
☐	Google Workspace Approved Sensitivity: High	9		Password 1 SAML 9	No issues found	a year ago	7 hrs ago	⋮
☐	LastPass Approved Sensitivity: High	9		Password 3 SAML 7	MFA not registered (3) Stolen credentials (2)	a year ago	7 hrs ago	⋮
☐	Okta Approved Sensitivity: High	9		Password 9	Leaked password (1) MFA not registered (8) Weak password (1)	a year ago	2 days ago	⋮
☐	Slack Approved Sensitivity: Medium	9		Password 9 OIDC 1	Leaked password (1) MFA not registered (5)	a year ago	2 days ago	⋮
☐	BambooHR Approved Sensitivity: High	7		SAML 7	No issues found	a year ago	7 hrs ago	⋮
☐	Loom Approved Sensitivity: Low	7		SAML 7	No issues found	a year ago	7 hrs ago	⋮
☐	OpenAI Approved Sensitivity: High	7		SAML 7	No issues found	a year ago	7 hrs ago	⋮

© Push 2025. All rights reserved. Privacy policy Terms



× App details

OpenAI
Website | Last used: 7 hrs ago

Owner

OpenAI is a language model platform that provides advanced natural language processing capabilities, enabling users to analyze and generate text-based content for various applications and tasks.

GenAI

Sensitivity level: High

Approval status: Approved

7 Employees

7 Accounts

First used: a year ago

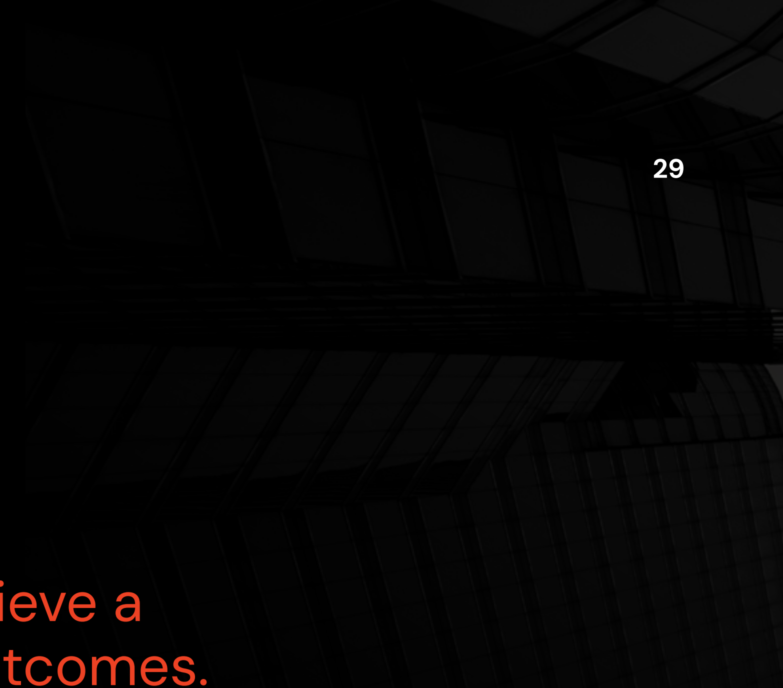
Push provides detailed data about third-party service usage, including which apps are used, by who, and how they are configured in terms of integrations, simplifying compliance reporting.

Data is provided in a dashboard view of the identity attack surface, with prioritized findings and can be exported via API, webhooks, or direct download to be used in conjunction with compliance reporting tools — enabling real-time streaming of compliance data.

You can use the dashboard to identify the sensitivity level of individual apps and set your own sensitivity levels and thresholds by user group, for granular management and control of app usage.

Push can be used to measure compliance with a range of security and compliance frameworks that have components relating to third party services and identity security, such as:

- **DORA**
- **GDPR**
- **HIPAA**
- **ISO 27001**
- **SOC 2**
- **NIST**



Key Outcomes

To summarize, Push enables security teams to achieve a range of key security, business, and compliance outcomes.

1.

Prevent, detect, and respond to identity attacks

By stopping attack techniques like phishing, AitM and BitM toolkit attacks, credential stuffing and session hijacking, Push enables you to prevent attackers from compromising your users' accounts and stop identity attacks at the earliest opportunity, before they can inflict harm on your organization.

2.

Map your entire identity attack surface

Push monitors your entire identity attack surface. Unlike other ITDR solutions that monitor only your managed identities that exist in your IdPs, Push discovers and monitors all your workforce identities. This includes unmanaged identities that can make up more than half of your overall identity attack surface.

3.

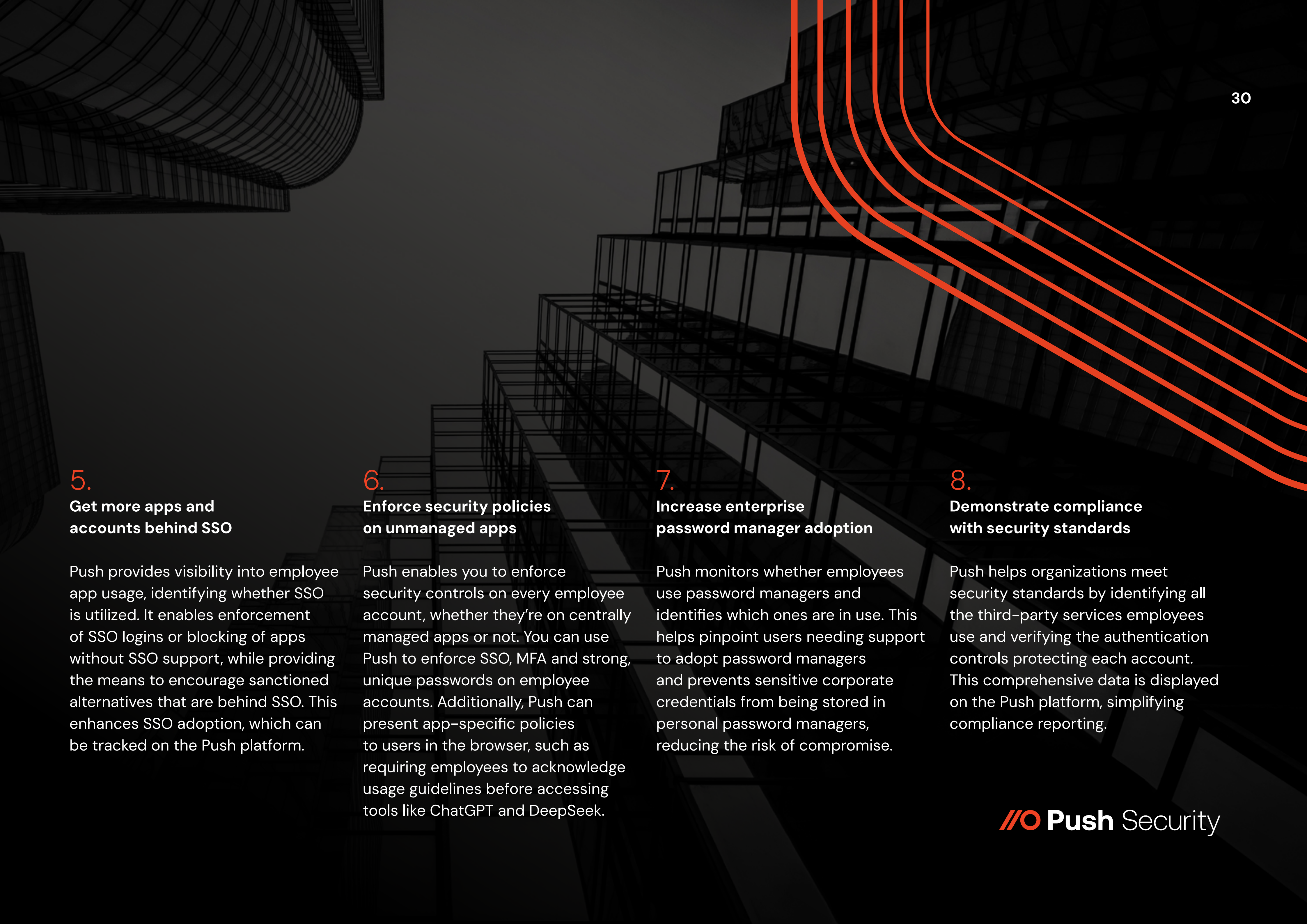
Find and fix identity vulnerabilities

Push surfaces vulnerabilities that can be exploited by common identity attack techniques. For example, employee accounts missing MFA and reusing the same password. The Push browser extension enables you to enforce stronger authentication controls at the point of login in the browser in order to harden workforce identities against common attack techniques.

4.

Create and manage your SaaS inventory

Push identifies all apps used by employees and compiles them into an app inventory, showing user activity, access methods, and potential security risks. It enables blocking of unsanctioned apps and in-browser guidance for secure app usage.



5.

Get more apps and accounts behind SSO

Push provides visibility into employee app usage, identifying whether SSO is utilized. It enables enforcement of SSO logins or blocking of apps without SSO support, while providing the means to encourage sanctioned alternatives that are behind SSO. This enhances SSO adoption, which can be tracked on the Push platform.

6.

Enforce security policies on unmanaged apps

Push enables you to enforce security controls on every employee account, whether they're on centrally managed apps or not. You can use Push to enforce SSO, MFA and strong, unique passwords on employee accounts. Additionally, Push can present app-specific policies to users in the browser, such as requiring employees to acknowledge usage guidelines before accessing tools like ChatGPT and DeepSeek.

7.

Increase enterprise password manager adoption

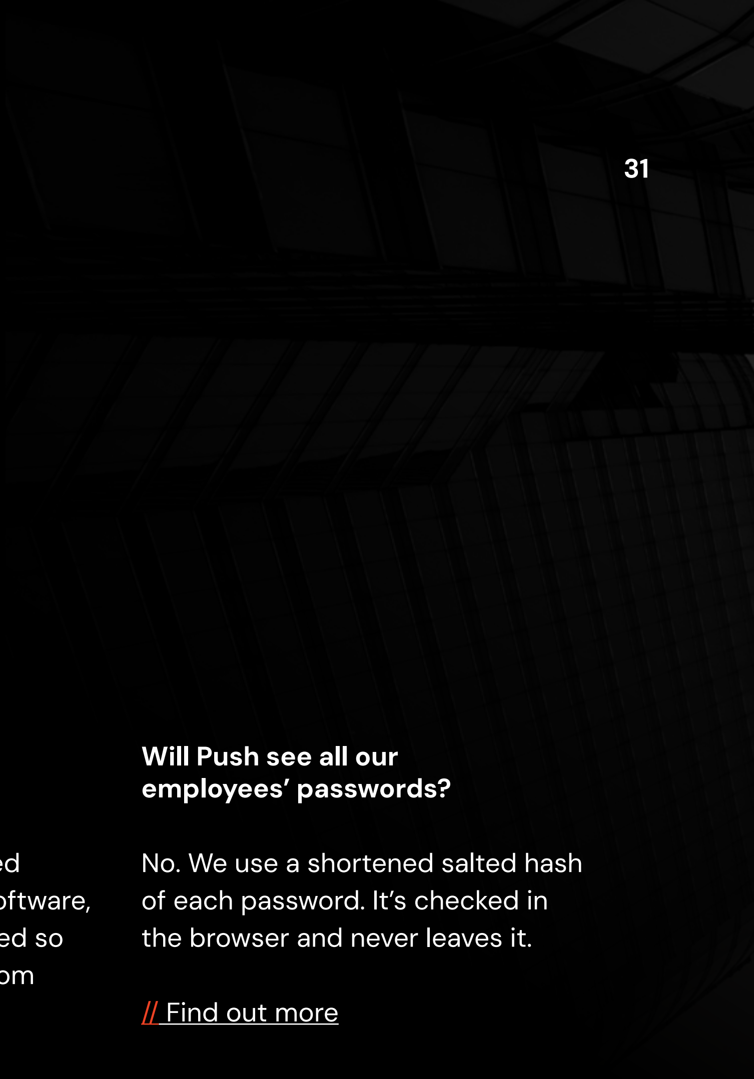
Push monitors whether employees use password managers and identifies which ones are in use. This helps pinpoint users needing support to adopt password managers and prevents sensitive corporate credentials from being stored in personal password managers, reducing the risk of compromise.

8.

Demonstrate compliance with security standards

Push helps organizations meet security standards by identifying all the third-party services employees use and verifying the authentication controls protecting each account. This comprehensive data is displayed on the Push platform, simplifying compliance reporting.

Push Security



FAQs

What browsers does Push support?

Google Chrome, Microsoft Edge, Firefox, Safari, Brave, Opera, Arc, and Island.

// Find out more

How do we deploy Push?

You can deploy the Push browser extension using managed browser configuration, an existing MDM solution (such as Jamf or Microsoft Intune), or through a Group Policy if you have an Active Directory environment.

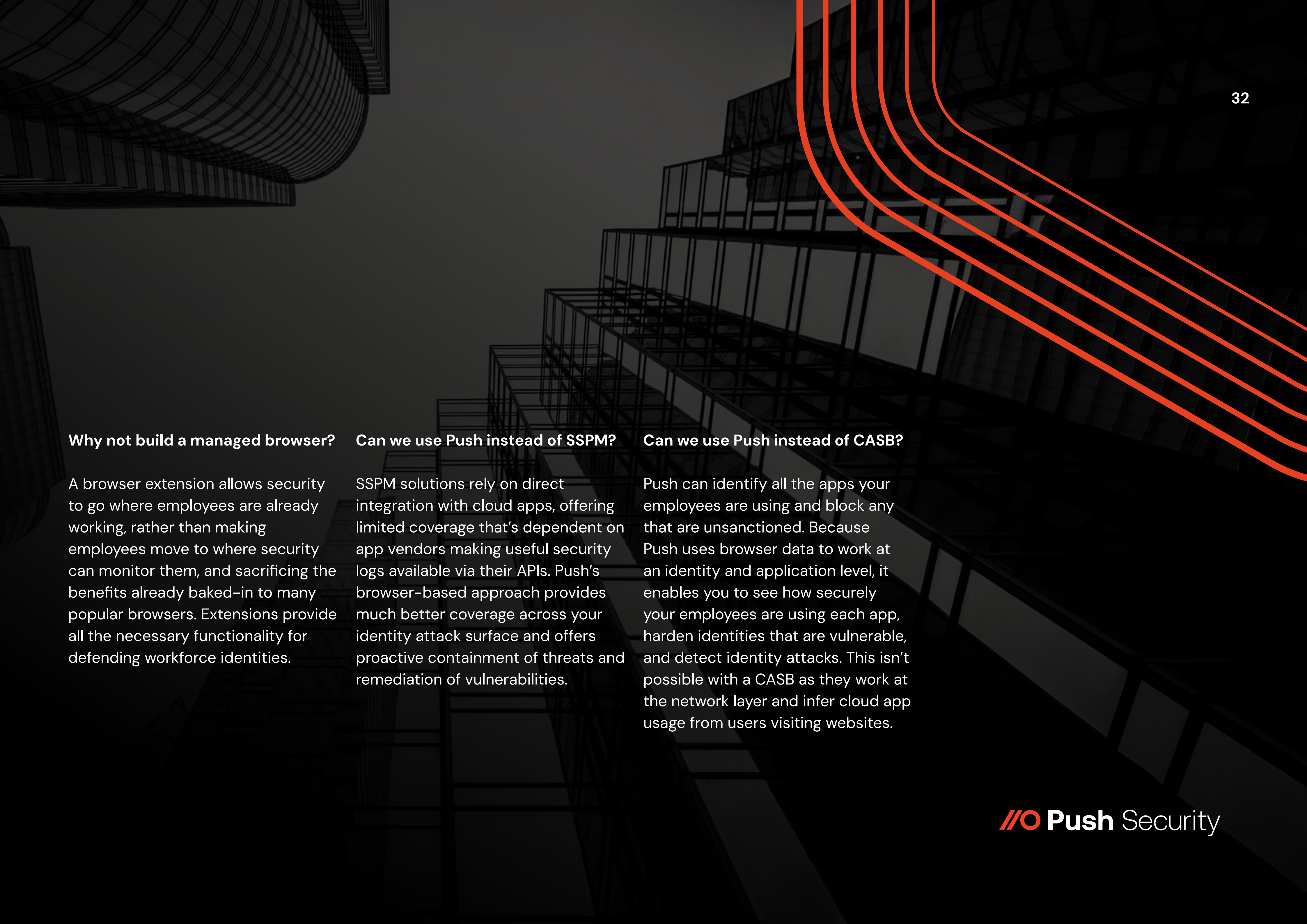
Can users remove the Push browser extension?

No, if the extension is installed using device management software, the extension can be deployed so that it cannot be removed from their browser.

Will Push see all our employees' passwords?

No. We use a shortened salted hash of each password. It's checked in the browser and never leaves it.

// Find out more



Why not build a managed browser?

A browser extension allows security to go where employees are already working, rather than making employees move to where security can monitor them, and sacrificing the benefits already baked-in to many popular browsers. Extensions provide all the necessary functionality for defending workforce identities.

Can we use Push instead of SSPM?

SSPM solutions rely on direct integration with cloud apps, offering limited coverage that's dependent on app vendors making useful security logs available via their APIs. Push's browser-based approach provides much better coverage across your identity attack surface and offers proactive containment of threats and remediation of vulnerabilities.

Can we use Push instead of CASB?

Push can identify all the apps your employees are using and block any that are unsanctioned. Because Push uses browser data to work at an identity and application level, it enables you to see how securely your employees are using each app, harden identities that are vulnerable, and detect identity attacks. This isn't possible with a CASB as they work at the network layer and infer cloud app usage from users visiting websites.

About Push Security

Push Security is built on a world-class combination of strategy, product, and above all cybersecurity leadership. Our team combines research-led offensive and defensive cybersecurity heritage with a proven commercial track record, with ex-MWR InfoSecurity, Duo Security, and CrowdStrike leaders.

ITDR, and Push's industry-first browser-based solution, is gaining increasing recognition from peers and investors. We're backed by Decibel Partners and Google Ventures, and count security leaders at Microsoft, Google, Thinkst, NCSC, Greynoise, and Sophos among our advisors and partners. Industry analysts agree that ITDR and an identity-first approach to security is essential for modern SecOps teams.

We're committed to developing awareness of the identity security problem space through our research and development. We're the creators of the widely used SaaS attack matrix on GitHub, our MITRE-inspired repository of identity and SaaS-native attack techniques.

Our researchers are regularly invited to speak at security conferences around the world, and we have a strong reputation for sharing the latest identity attack research, which has been covered in various security media, news sites, and podcasts.

All this research informs the development of new detections and controls, so you can stay one step ahead of adversaries using the latest identity attack techniques.

To learn more, check out our website at pushsecurity.com and book a demo to find out how Push extends your threat detection and response capabilities into the browser and across your identity attack surface.

> // Push Security is like EDR, but for your identities. //
>
> **Geoff Belknap**
>
> CVP, Deputy CISO (Core and M&A) Microsoft
> Former LinkedIn, Slack, Palantir

Scan to book a demo

Investors and advisors

Jon Oberheide
Co-Founder & former CTO
Duo Security

Dug Song
Co-Founder & former CEO
Duo Security

Geoff Belknap
Deputy CISO
Microsoft

Royal Hansen
CISO
Alphabet

Haroon Meer
Founder
Thinkst

Ollie Whitehouse
Former CTO
NCC Group

Ross McKerchar
CISO
Sophos

John Viega
Founder & former CEO
Capsule8

> *"Organizations increasingly recognize the need for specialized ITDR tools, positioning Push Security as a critical component of modern cybersecurity strategies. Its compatibility with Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) solutions further enhances its relevance and adoption.*
>
> *We anticipate continued convergence within the ITDR space, with increased integration of ITDR signals into broader SIEM and XDR ecosystems. Solutions like Push Security's, which provide unique telemetry and enhance cross-platform visibility, are poised to become integral to cybersecurity strategies. As the market matures, we expect greater consolidation and the emergence of unified platforms delivering end-to-end identity protection."*

KuppingerCole
ANALYSTS

101 Arch Street
8th Floor
Boston, MA 02110

www.pushsecurity.com

Push Security